

Políticas de Seguridad Informática - Mejores Prácticas Internacionales

Conjunto Completo de
Políticas de Seguridad Informática

Versión 9.0

CHARLES CRESSON WOOD, CISA, CISSP



NetIQ, Inc.

Cómo Entender las Políticas de Seguridad Informática

por Charles Cresson Wood, CISA, CISSP

© 2000-2002 NetIQ, Inc. Todos los derechos reservados.
Impreso en los Estados Unidos de América.

Publicado por NetIQ, Inc., 1233 West Loop South #1800, Houston, TX 77027.

Editor Asesor: Scott Hayden, CISA, CISSP

Editor Técnico: Steven W. Martinson

Editor de Texto: Nadja Pollard

Gerente de Producción: Liz Carter

Diseño de Cubierta: Krista Kirkland

Ediciones Anteriores: Septiembre 2002: Primera Edición.

Versión Autorizada en Castellano elaborada por Scientech de Venezuela C.A, con la colaboración de Scientech de Colombia S.A y Scientech infocom Inc.; www.scientechsecurity.com; Julio 2003:

Editor Técnico en Castellano: Ing. Luis Daniel Riveros. LRiveros@scientech.com.ve

Gerente de Producción para Versión Castellana: Tony J. de Castro; TdeCastro@scientechsecurity.com.

© Copyright, NetIQ, Inc., Todos los derechos reservados, Septiembre, 2002.

El derecho a utilizar el material de este manual y sus medios de almacenamiento (CD-ROM, discos, etc.) se otorga solamente a los compradores registrados con licencia, tal como se describe en la página inicial de este manual.

La información contenida en este manual de referencia y sus medios de almacenamiento relacionados se proporciona como un servicio a la comunidad empresarial. Al momento de su preparación, las políticas y los otros materiales contenidos en este manual se consideraban actuales, relevantes, útiles y apropiados para las organizaciones preocupadas por la seguridad informática. Dicha información está, sin embargo, sujeta a cambio sin previo aviso. Aunque se han realizado todos los esfuerzos razonables para garantizar la exactitud, totalidad y relevancia de la información aquí contenida, el autor y la casa editora (NetIQ, Inc.), inclusive de sus afiliados, no pueden ser responsables de cualesquiera errores y omisiones, o de las interpretaciones o aplicaciones que haga cualquier persona de las ideas o palabras aquí contenidas. Se recomienda a los lectores que preparan políticas y materiales relacionados, obtener la asesoría de abogados experimentados en asuntos de tecnología informática, así como de especialistas técnicos en el área de seguridad informática. Ni el autor ni Pentasafe Security Technologies Inc., ni cualquiera de sus afiliados, otorga garantías ni representaciones de clase alguna acerca de lo apropiado que puedan resultar para propósito alguno las políticas de seguridad informática y su material relacionado aquí incluido.

Este manual se vende en copias individuales separadas. La licencia específica de una organización para copiar, modificar y re-publicar partes de este manual como documentación propia se otorga solamente a los compradores registrados para uso interno solamente. Este material es sólo para el uso interno de las organizaciones que ya hayan recibido su licencia y no puede ser remercadeado o redistribuido. Los consultores, VARs, OEMs, y otras terceras partes que utilicen este material a nombre de otra organización deben adquirir licencias separadas para cada organización donde se utilice este material.

Ninguna parte de este material puede ser reproducida o transmitida de cualquier método o manera o vía, sea electrónica o mecánica, incluyendo el fotocopiado, la grabación, o cualquier otro sistema de almacenamiento, sin el consentimiento escrito del propietario del derecho de autor, excepto donde lo permita la ley.

*A Andi, por su visión
de lo que pudiera ser.*



CONTENTS

Introducción	1
Instrucciones	5
Instrucciones	5
Políticas de Seguridad Informática	5
Importancia de las Políticas	7
Pasos para el Desarrollo de las Políticas	12
Cronograma para el Desarrollo de las Políticas	22
Longitud del Documento de Políticas	23
Utilización de las Políticas	30
Objetivos y Alcance de las Políticas	31
Excepciones de Responsabilidad	35
Políticas Específicas	37
Política de Seguridad	37
3.01 Política de Seguridad Informática	37
Seguridad Organizacional	41
4.01 Infraestructura de la Seguridad Informática	41
4.02 Seguridad en el Acceso de Terceros	53
4.03 Contratos Externos de Servicio	64
Clasificación y Control de Activos	69
5.01 Responsabilidad por Activos	69
5.02 Clasificación de la Información	73
El Personal	97
6.01 La Seguridad en Definiciones de Trabajo y Contratación	97
6.02 Adiestramiento de Usuarios	117
6.03 Respuesta a Incidentes y Anomalías de Seguridad	123
Seguridad Física y Ambiental	138
7.01 Areas Seguras	138
7.02 Seguridad de los Equipos	152
7.03 Controles Generales	162
Gestión de Operaciones y Comunicaciones	166
8.01 Responsabilidades y Procedimientos Operativos	166
8.02 Planificación y Aceptación del Sistema	181
8.03 Protección Contra Software Malicioso	186
8.04 Mantenimiento	195
8.06 Manejo y Seguridad de Medios de Almacenamiento	219
8.07 Intercambio de Información y Software	231
Control de Acceso	301
9.01 Requisitos para el Control de Acceso	301
9.02 Administración del Acceso de Usuario	313
9.03 Responsabilidades del Usuario	329
9.04 Control de Acceso a la Red	338
9.05 Control de Acceso al Sistema Operativo	351
9.06 Control de Acceso a las Aplicaciones	371
9.07 Monitoreo del Acceso y Uso del Sistema	378
9.08 Computación Móvil	390

Desarrollo y Mantenimiento de Sistemas	397
10.01 Requerimientos de Seguridad de los Sistemas	397
10.02 Seguridad en Sistemas de Aplicaciones	402
10.03 Controles Criptográficos	410
10.04 Seguridad de los Archivos del Sistema	425
10.05 Seguridad en los Procesos de Desarrollo y Soporte	427
Gestión de Continuidad de Negocio	438
11.01 Aspectos de Gestión de Continuidad de Negocio	438
Cumplimiento	444
12.01 Cumplimiento de Requisitos Legales	444
12.02 Revisión de Políticas de Seguridad y Cumplimiento Técnico	501
12.03 Consideraciones sobre Auditoría de Sistemas	504
Modelo de Política de Seguridad Informática de Alto Nivel	507
Modelo de Política de Seguridad Informática Detallada	515
Modelo de Política de Seguridad en Teletrabajo y Equipos Móviles	529
Asuntos Gerenciales	529
Control de Acceso	530
Respaldo y Almacenamiento de Medios	530
Enlaces de Comunicaciones	531
Administración del Sistema	532
Consideraciones en Traslados	533
Seguridad Física	533
Modelo de Política de Seguridad en Comunicaciones Externas	535
Modelo de Política de Seguridad de Computadores Personales	541
Bosquejo del Documento	541
Sólo Para Uso Empresarial	541
Control de la Configuración	541
Control de Acceso	542
Virus	542
Respaldo	543
Destrucción	543
Documentación	544
Trabajo en Redes	544
Seguridad Física	545
Gestión	546
Modelo de Política de Correo Electrónico	549
Modelo de Política de Seguridad en Redes de Computación	555
Propósito	555
Alcance	555
Política General	555
Responsabilidades	555

Control de Acceso al Sistema	556
Contraseñas de los Usuarios Finales	556
Instalación y Configuración del Sistema de Contraseñas	557
Proceso de Inicio y Cierre de Sesión	558
Privilegios en el Sistema	558
Establecimiento de Vías de Acceso	560
Virus, Gusanos y Caballos de Troya	561
Respaldo de Programas y Datos	561
Cifrado	562
Computadores Portátiles	562
Impresión Remota	563
Privacidad	563
Registros y Otras Herramientas de Seguridad en Sistemas	563
Manejo de la Información de Seguridad de la Red	564
Seguridad Física de los Equipos de Computación y de Comunicaciones	564
Excepciones	565
Violaciones	565
Glosario	565
 Modelo de Política de Seguridad en Internet para Usuarios	569
Introducción	569
Integridad de la Información	569
Confidencialidad de la Información	570
Representaciones Publicas	571
Derechos Sobre la Propiedad Intelectual	571
Control de Acceso	572
Uso Personal	573
Expectativas de Privacidad	573
Reportes de Problemas de Seguridad	574
 Modelo de Política de Seguridad en Intranets	575
 Modelo de Política de Privacidad — Estricta	577
Bosquejo y Aplicabilidad	577
Definiciones	577
Requerimientos Específicos	578
Información a Suministrar a la Persona	579
Derecho de las Personas a Acceder a los Datos	580
Derecho de la Persona a Objeter	580
Divulgación de Datos Personales a Terceros	580
Confidencialidad y Seguridad del Procesamiento	581
Monitoreo de Actividades Internas	582
 Modelo de Política de Privacidad — No Estricta	583
Intención de la Empresa y Responsabilidad de la Gerencia	583
Divulgación de Información Privada	583
Manejo Correcto de la Información Privada	584
Información Privada en Sistemas de Computación y de Comunicaciones	584
Monitoreo de las Actividades	585
Manejo de la Información del Personal	586
Información Privada de Solicitantes de Empleo	586
Información Privada de Clientes	586

Modelo de Política de Privacidad en la Web	589
Modelo de Política de Clasificación de Datos	591
Introducción y Bosquejo	591
Control de Acceso	592
Etiquetas de Clasificación	592
Etiquetado	593
Interacciones con Terceros	594
Manejo y Envío	595
Desclasificación y Degradación	596
Destrucción y Disposición	597
Seguridad Física	598
Consideraciones Especiales en Información Secreta	598
Modelo de Tabla de Referencia Rápida de Clasificación de Datos	601
Modelo de Política para la Divulgación de Información a Terceros	605
Determinar si la Divulgación es Apropriada	605
Resolución de Problemas en los Procesos de Divulgación	606
Registro Obligatorio de la Divulgación	607
Preparación de la Información para su Divulgación	607
Modelo de Política de Propiedad de la Información	609
Modelo de Política de Cortafuegos	613
Lista de Referencias para las Políticas de Seguridad Informática	617
Lista de Publicaciones Periódicas Sobre Seguridad Informática	619
Lista de Asociaciones Profesionales y Organizaciones Relacionadas	623
Genéricas	623
Por Industria	625
Por Segmento de Mercado	626
Lista de Métodos Sugeridos para Aumentar Nivel de Conciencia	627
En Persona	627
Por Escrito	628
En Sistemas	629
.....	631
Por Otras Vías	631
Armonización de las Políticas de Seguridad con Interfaces Externas de Red	633
Consideraciones en Control de Acceso	634
Consideraciones en Cifrado y en Infraestructura de Clave Pública	634
Consideraciones en Control de Cambios y Planificación de Contingencias	635
Consideraciones en Gestión de Redes	635
Lista de Verificación de Pasos en Proceso de Desarrollo de Políticas	637
Vista General de las Tareas del Proceso de Desarrollo de las Políticas	639

Problemas Reales Ocasionados por la Ausencia de Políticas	641
Agencia Gubernamental	641
Bufete de Abogados	641
Empresa Petrolera	641
Periódico Local	641
Empresa Manufacturera del Medio Oeste Norteamericano	642
Empresa Manufacturera de la Costa Oeste Norteamericana	642
Empresa Importante de Servicios en Línea	642
Sugerencias para los Próximos Pasos	643
Convenio de Cumplimiento de las Políticas de Seguridad Informática	647
Declaración de Responsabilidad sobre la Tarjeta de Identidad	649
Declaración de Aceptación de Riesgo	651
Cuándo Utilizar Este Formulario	651
Acuerdo Simple de Confidencialidad	655
Indice de Nuevas Políticas	657
Indice de Nuevos Nombres de Políticas	667
Acerca del Autor	747

Capítulo 1 INTRODUCCIÓN

Las políticas de seguridad informática representan un tipo especial de reglas de negocios documentadas. Hace 25 años no existía tal necesidad de políticas, pero el cambio ha sido estimulado por la explosión de tecnologías de manejo de información, incluyendo a los teléfonos celulares, los buscaperonas y los computadores. Los que trabajan en el ambiente empresarial deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información generada en el complejo mundo de los negocios. Así como es inconcebible pensar que millones de conductores de automóviles puedan conducir sin leyes de tránsito, es también difícil pensar que millones de personas de negocios pudieran operar sistemas sin políticas de seguridad informática.

Afortunadamente, la alta gerencia de muchas organizaciones ha empezado a entender la importancia de las reglas de negocio, tales como las políticas de seguridad informática, porque a su alrededor existen proyectos que dependen de manera crítica de un sistema con reglas claramente articuladas. Por ejemplo, algunos altos gerentes pueden recordar el momento cuando una aplicación importante fue migrada desde el mainframe hasta Internet, y uno de los pasos importantes que permitió esta transición fue la documentación adecuada de las reglas de negocio. Sin dichas reglas claras de negocio, los creadores de nuevos sistemas no pueden estar seguros de que lo que están construyendo funcionará tal como lo espera la gerencia. Igualmente, sin políticas de seguridad informática, la gerencia no puede garantizar que los sistemas informáticos son operados de manera segura.

Desde el punto de vista histórico, siempre se ha pensado que los que trabajan en el campo de la seguridad informática disminuyen la velocidad de los procesos. Algunos hasta habían dicho que la seguridad informática no era compatible con el rápido avance empresarial que exigía la nueva economía basada en Internet. Pero este punto de vista fue cambiando con rapidez a medida que la gente ha notado que el negocio de Internet no sería posible a menos que la organización hiciera un buen trabajo en el área de seguridad informática. El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación de la organización. Ahora, en cambio, la seguridad informática está

siendo considerada como un acelerador de procesos. Si una organización puede codificar sus reglas de negocio y sus procesos internos, puede también automatizar o contratar externamente estos reglamentos y procesos, e iniciar nuevas relaciones basadas en ellos para dirigirse hacia nuevos destinos. Para todos estos proyectos y muchos otros, las políticas de seguridad informática proporcionan delimitaciones claras que definen un dominio donde se puede encontrar una solución aceptable.

Cada día es más evidente la necesidad de centralizar las políticas de seguridad informática para cubrir virtualmente todo lo que sucede en dicho campo. Por ejemplo, los administradores de sistemas no pueden instalar con seguridad un cortafuego, a menos que hayan recibido un grupo de políticas claras, porque ellas estipulan el tipo de servicios de transmisión a permitir, cómo autenticar las identidades de los usuarios y cómo llevar un registro de los eventos relativos a la seguridad. Tampoco se puede iniciar un adiestramiento efectivo sobre la seguridad informática y sobre el esfuerzo de concientización que al respecto se requiere, sin documentar las políticas de seguridad informática, porque dichas políticas proporcionan el contenido esencial del adiestramiento mismo.

Existen muchas otras importantes razones para disponer de políticas de seguridad informática. Por ejemplo, las políticas son importantes documentos de referencia para auditorías internas y para la resolución de disputas legales acerca de la debida diligencia de la gerencia. Por otra parte, existen indicios de que los documentos de políticas pueden servir de demostración de la intención original de la gerencia y, por lo tanto, reducir su potencial responsabilidad legal, e inclusive pueden utilizarse como evidencia de las intenciones gerenciales de salvaguardar información intelectual. Este es un paso esencial pero desatendido en la protección de los secretos industriales. Igualmente, las políticas de seguridad informática pueden ser evidencia de los procesos de control de calidad, lo cual puede conferir a un socio la suficiente confianza como para suministrar material confidencial, así como asistir en un proceso de certificación de control de calidad ISO 9000.

Si bien es cierto que algunos desarrollos recientes en tecnologías de seguridad informática, tales como los certificados digitales, son impresionantes y prometen mucho, también es cierto que lo mejor en materia de

seguridad informática es relativamente nuevo y muchas de las cosas que hacen falta no pueden lograrse a buena relación costo-valor con la tecnología existente. Por ejemplo, un rótulo o etiqueta de clasificación de datos no puede fijarse permanentemente a una pieza de información con la intención de que permanezca siempre con la información aunque ésta sea resumida, editada, reformateada, retranscrita, o incorporada a otra. Así que reconocer las limitaciones de la tecnología es un paso importante en el proceso de entender la importancia de las políticas. Dado que existen tantas cosas que no pueden lograrse a buen costo con las herramientas tecnológicas actuales, éstas deben ser realizadas por humanos. Las políticas, entonces, proporcionan la fuente de instrucciones más importante y más frecuentemente referenciada que detalla cómo los trabajadores pueden proteger tanto la información como los sistemas que la contienen.

Algunos dicen que la seguridad informática es un problema de personas, mientras que otros dicen que es un problema de tecnología, y podría decirse que ambos tienen razón. Pero antes de que se pueda hacer algo al respecto, la gerencia debe involucrarse en la seguridad informática, asignar suficientes recursos y comunicar claramente a todos los integrantes de su equipo que la seguridad informática realmente sí es importante. Por ello se afirma que, en el fondo, la seguridad informática es un problema de gerencia. Muchas encuestas indican que aquéllos que ejercen la seguridad informática piensan que la llave para alcanzar el éxito de la seguridad informática es la participación de la alta gerencia. Al redactar una política de seguridad informática, la alta gerencia debe iniciar conversaciones sobre las necesidades especiales de la organización, porque a través de ellas es que se pueden abrir los ojos para ver la verdadera importancia y lo crítico que resulta la seguridad informática. Para mayor información sobre el uso de las políticas de seguridad informática, ver Capítulo 2, “[Instrucciones](#).”

Dado que las políticas tienen tan profundo impacto en cualquier esfuerzo de seguridad informática, es importante que las políticas sean claras y suficientes, y que respondan a los sistemas informáticos. Aun cuando este manual puede proporcionar un punto de partida para casi cualquier organización, las políticas tendrán que ser adecuadas a las circunstancias particulares de cada una de ellas. Aparte de esta adecuación, los especialistas de seguridad informática deben hacer una re-examinación periódica de las políticas a fin de determinar si necesitan modificarse. Este manual tiene

el propósito de presentarse como una referencia para apoyar tanto a los practicantes y redactores de políticas, como a aquellos que las reescriben o expanden.

Sin importar el tamaño de la organización, la industria de la que forme parte, su situación geográfica, o hasta qué punto utilice computadores, la seguridad informática es un asunto importante que debe atenderse a través de políticas explícitas. Algunos expertos dicen que la falta de una política de seguridad informática corporativa bien definida es el problema más grande que enfrenta cualquier esfuerzo que se realice en esta área. Por ello, este manual proporciona ejemplos concisos de políticas que pueden adaptarse rápidamente a las necesidades de cualquier organización.

Aunque nos encantaría que fuese de otra manera, las políticas simplemente no pueden sacarse de un estante, redactarse, aprobarse mediante un fácil proceso burocrático y emitirse, sino que deben adaptarse a las necesidades específicas de cada organización. Esto se debe a que los factores que impulsan las políticas de seguridad informática varían considerablemente de organización en organización. Dichos factores incluyen los objetivos comerciales, los requisitos legales, el diseño organizacional, la cultura organizacional, la ética y las buenas costumbres, el nivel educativo del trabajador y la tecnología utilizada en los sistemas informáticos.

Sin embargo, las ideas que sustentan las políticas de seguridad informática sí son similares en las distintas organizaciones. Este manual proporciona el contenido esencial que debe formar parte de las declaraciones de política. Pero, para que dicho contenido se adapte a una organización en particular, es necesario que el lector esté familiarizado con los factores descritos en el párrafo anterior. Quizás la mejor manera de familiarizarse con estos factores es a través de una evaluación de riesgo. Para más información sobre este tema, ver Capítulo 2, “[Instrucciones](#).”

Este manual incluye casi todas las políticas ahora consideradas parte de la norma de debido cuidado profesional no militar en seguridad informática. La norma de debido cuidado profesional define el conjunto mínimo de medidas de seguridad informática que se espera en una organización, sin importar el tipo de industria a la que pertenezca. En este material se han incluido muchas políticas adicionales que van más allá de esta norma de debido cuidado, porque proporcionan un nivel más riguroso de seguridad. Se agregan estas políticas adicionales para brindar al lector un juego más completo de opciones a las cuales hacer referencia al momento de preparar su borrador de políticas de

seguridad informática. Cada organización debe adoptar una combinación de políticas; algunas de las incluidas en la norma de debido cuidado y otras de las adicionales aquí proporcionadas.

Si bien la norma de debido cuidado es ampliamente aceptada y apoyada, desafortunadamente no existe en la actualidad una norma mundial que defina las políticas específicas de seguridad informática. El más cercano es el documento número 17799 de la Organización Internacional de Normas y Estándares (ISO), el cual define un esquema y proporciona orientación de alto nivel sobre políticas de seguridad informática. Las

políticas de este manual están organizadas sobre la base del esquema ISO 17799. Dada la rapidez de significativos desarrollos en las áreas legales, empresariales e informáticas, todavía mucha gente se pregunta si alguna vez tendremos un conjunto específico de políticas normalizadas a nivel internacional. Mientras tanto, este manual y su CD-ROM anexo proporcionan la colección más completa de políticas en todo el mundo. Es responsabilidad de cada lector determinar cuáles de estas políticas se pueden aplicar a una organización específica.



Capítulo 2 INSTRUCCIONES

INSTRUCCIONES

Esta sección proporciona la orientación necesaria para acometer el proceso de redacción de las políticas de seguridad informática. Aunque puede ser tentador comenzar de inmediato recortando y pegando algunas de las políticas aquí contenidas, lo ideal sería leer estas instrucciones primero, porque proporcionan el material de sustentación requerido para que todas las tareas subsiguientes de redacción de las políticas fluyan con más eficacia y con el enfoque adecuado.

Esta sección brinda orientación precisa sobre el complejo proceso de desarrollo de las políticas de seguridad informática. Dicho proceso incluye la redacción de las políticas y su corrección, la obtención de la autorización de la gerencia, la divulgación de las políticas y la implantación de los controles necesarios. Las últimas subsecciones contienen ayuda y sugerencias de cómo obtener el mayor provecho de este manual y del material computacional anexo.

Políticas de Seguridad Informática

Políticas Versus Lineamientos y Normas

Las políticas son instrucciones gerenciales que trazan una dirección predeterminada o describen la manera de manejar un problema o situación. Las políticas son planteamientos de alto nivel que transmiten a los trabajadores la orientación que necesitan para tomar decisiones presentes y futuras. Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas dentro, y en algunos casos fuera, de la organización. Las políticas también pueden considerarse como reglas de negocio. Aunque los documentos de políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de las políticas.

Las políticas son obligatorias y pueden considerarse el equivalente de una ley propia de la organización. Se requiere una autorización especial cuando un empleado desea irse por un camino que no está contemplado en la política. Debido a que el cumplimiento es obligatorio, las políticas utilizan palabras como "no se debe hacer" o "se tiene que hacer", ya que estas estructuras semánticas transmiten certeza e indispensabilidad. Por razones de simplicidad y uniformidad, se emplea el verbo "deber" en todo el manual, pero cualquier equivalente es aceptable.

Las políticas son similares a los lineamientos, pero éstos representan sólo opciones y recomendaciones. Las políticas de este manual pueden ser transformadas en lineamientos, simplemente reemplazando el verbo "deber" con el potencial "debería". Sin embargo, no se recomienda la transformación de las políticas en lineamientos, porque los lineamientos violan el principio básico de diseño de sistemas seguros; es decir, que el producto tiene que ser "de aplicación universal". Esto significa que los controles son significativamente débiles si no son aplicados de manera consistente. Los lineamientos son deseables en algunos casos. Por ejemplo, cuando un trabajo debe hacerlo un grupo distribuido de individuos que no puede ser obligado a cumplir una política, entonces el departamento encargado de la seguridad informática puede emitir lineamientos en lugar de políticas. Este enfoque es común, por ejemplo, en la preparación de planes de contingencia por departamento de acuerdo con los lineamientos emitidos por un grupo de seguridad informática centralizado.

Las políticas representan declaraciones instrucionales de más alto nivel que las normas, aunque ambas son de obligatorio cumplimiento. Las políticas proporcionan las instrucciones generales, mientras que las normas indican requisitos técnicos específicos. Las normas cubren detalles como, por ejemplo, los pasos a seguir para lograr alguna implementación, los conceptos del diseño de los sistemas, las especificaciones de las interfaces del software, los algoritmos y otros. La frase "arquitectura de la seguridad informática" está ganando terreno como el conjunto aceptado de normas integradas

de seguridad informática. las normas, por ejemplo, definirían la cantidad de bits de la llave secreta que se requieren en un algoritmo de cifrado. Por otro lado, las políticas simplemente definirían la necesidad de utilizar un proceso de cifrado autorizado cuando se envíe información confidencial a través de redes públicas, tales como Internet.

Las políticas están diseñadas para durar hasta cinco años, mientras que las normas sólo unos pocos. Las normas necesitan modificarse más a menudo debido al cambio incesante en los procedimientos manuales, en las estructuras organizacionales, en los procedimientos empresariales y en la tecnología de sistemas informáticos. Por ejemplo, una norma de seguridad de la red podría especificar que todos los sistemas nuevos o sustancialmente modificados tienen que satisfacer la norma X509 de la Organización de Normas Internacionales (International Standards Organization, ISO), que consiste en la autenticación de un canal de comunicaciones seguro mediante criptografía de clave pública. Lo más probable es que esta norma sea revisada, ampliada o reemplazada en pocos años.

Las políticas generalmente van dirigidas a un público más amplio que las normas. Por ejemplo, una política que exija la utilización de paquetes antivirus se aplicaría a todos los usuarios de computadores personales, pero la norma que requiera el uso de certificados digitales de clave pública sólo podría ser dirigido al personal que realice operaciones a través de Internet.

Políticas Versus Procedimientos y Controles

Las políticas no sólo son distintas, sino que se encuentran a un nivel mucho más alto que los procedimientos. Algunas veces se denominan procedimientos operativos normativos o procedimientos operativos departamentales. La declaración de una política describe los lineamientos generales que deben seguirse para atender un problema específico, mientras que los procedimientos dictan los pasos operativos específicos o los métodos manuales que los trabajadores deben emplear para lograr un objetivo dado. Por ejemplo, en muchos departamentos de tecnología informática existen procedimientos específicos para realizar los respaldos de los discos duros de los servidores. En este ejemplo, la política podría plantear o describir la necesidad de realizar respaldos, de tener almacenaje fuera de la sede y de salvaguardar los medios de respaldo. La norma podría definir el software a utilizar para hacer los respaldos y cómo configurar dicho software. El procedimiento podría describir cómo usar el software de respaldo, cómo y cuándo sincronizar dichos respaldos y otros detalles.

La Norma de Calidad ISO 9000 de la Organización Internacional de Normas (ISO) para la preparación de documentos internos, enfatiza la necesidad de diferenciar claramente entre las políticas, las normas y los procedimientos. Por ejemplo, estas normas de la ISO explícitamente establecen que las políticas tienen que estar separadas y diferenciadas de los procedimientos. En algunas organizaciones, las políticas se hacen detalladas y largas, y en el proceso de desarrollo se transforman en una combinación confusa de políticas y procedimientos. Aunque es útil y altamente recomendable una clara demarcación entre estos tipos de documentos, nada de lo expuesto aquí hasta ahora implica que estos documentos no pueden coexistir en una misma carpeta o enlazadas dentro de un sitio de documentación en la Intranet de la organización.

Pero peor aún es combinar políticas, normas y procedimientos en un solo documento. Llegado el momento de actualizar tal documento, el procedimiento consume demasiado tiempo y al final resulta confuso. Esto se debe a que estos tres tipos de documentos tienen distintos niveles de detalle y tratan asuntos diferentes. Además, como están dirigidos a distintos públicos, se corre un alto riesgo de que el material no sea leído. La gente no tiene tiempo y, si el documento contiene mucho material que no les es relevante, probablemente no lo leerán. Tampoco es recomendable la combinación de políticas, normas y procedimientos en un solo documento debido a que al lector se le hace difícil ubicar la información que le interesa. Este enfoque de combinación es también ineficaz en términos de distribución de la información, porque envía mucha a quien no la necesita. Así que si quiere simplificar el mantenimiento del material, el uso y las referencias cruzadas, asegúrese de crear documentos separados para las políticas, las normas y los procedimientos.

Las políticas son diferentes de los controles, también conocidos como contramedidas, medidas de seguridad y salvaguardas, porque el control es un dispositivo o un mecanismo usado para regular o guiar la operación de una máquina, aparato, sistema o proceso. Un ejemplo de un control sería el cifrado de los datos confidenciales contenidos en un disco flexible. En muchos casos, las políticas proporcionan objetivos amplios que sólo se pueden cumplir si existen los controles adecuados. Por ejemplo, una política que prohíba conflictos de intereses, tanto los reales como los aparentes, podría satisfacerse parcialmente a través de un control que exija a los empleados firmar una declaración donde indique que ellos han leído el código de conducta y que convienen en cumplirlo. Igualmente, muchas veces, las medidas de control son dictadas directamente por la

política. Por ejemplo, el requisito de firmar una declaración de cumplimiento del código de conducta es, en sí mismo, una política.

Importancia de las Políticas

Con la cobertura que los medios noticiosos brindan a la Seguridad Informática, cualquiera pensaría que la gerencia entiende lo que es una política de Seguridad Informática y por qué es necesaria. Lamentablemente, no es así. Por eso, antes de redactar un documento de política hay que consultar a la gerencia y garantizar que todos hablan el mismo idioma y que ellos entienden por qué es importante este esfuerzo para desarrollar las políticas.

La subsección anterior, “[Políticas de Seguridad Informática](#)”, aporta palabras específicas que podrían formar parte de un memorando escrito con el propósito de clarificar los resultados del trabajo. Los modelos de políticas ubicados al final de este manual también pueden presentarse a la gerencia como bosquejos aproximados de los productos finales a ser producidos. La siguiente sección aporta ideas específicas que pueden formar parte de un memorando con razones detalladas explicando por qué es importante una política de Seguridad Informática. La Tabla 1 muestra un resumen de las razones que justifican la adopción de políticas de Seguridad Informática. Algunas de las razones de mayor importancia para desarrollar políticas de seguridad informática se describen en sus propias subsecciones, inmediatamente después de la próxima subsección.

Garantía de Implementación de los Controles

La gerencia adquiere uno o más productos de Seguridad Informática con la firme esperanza de manejarla rápida y fácilmente porque piensa que los nuevos productos, tales como el hardware, el software, el contenido de la información o de los servicios, es todo lo que necesita. Poco después de instalar los productos, la gerencia se decepciona al darse cuenta que los resultados no se materializan. Muchas veces, sin embargo, esta decepción tiene su origen en la falta de la gerencia porque no estableció una infraestructura organizacional adecuada para mantener la Seguridad Informática. Y uno de los componentes cruciales de dicha infraestructura es el documento de políticas.

Veamos un ejemplo claro de este punto. Supóngase que una gran organización recientemente adquirió un paquete de control de acceso único para un súper servidor multiusuario conectado a la Intranet. La sola instalación de este paquete mejorará poco la seguridad, porque la gerencia tiene que decidir a cuáles usuarios debe dar acceso a cuáles recursos, preferiblemente a través de una política. Luego debe establecer los procedimientos que debe seguir el personal técnico para configurar los controles de manera consistente con esas decisiones. Y después, la gerencia debe definir las formas de revisar los registros generados por el paquete de control de acceso. Estos y otros esfuerzos constituyen sólo una parte de la infraestructura organizacional necesaria para apoyar los productos de seguridad. La mayoría de los proveedores de tecnología no proporcionan políticas, procedimientos ni otros aditamentos necesarios para el uso inmediato de sus productos. La organización misma tiene que desarrollar una infraestructura organizacional, por cuanto la infraestructura responde y depende de los requerimientos particulares de cada organización.

Para establecer una infraestructura organizacional de apoyo, cada organización necesita desarrollar varios documentos, incluyendo las declaraciones de responsabilidad organizacional, las políticas, las normas, los procedimientos operativos y los mecanismos de cumplimiento. También se necesitan varios procesos gerenciales, incluyendo el proceso de evaluación de riesgos, el proceso para coordinar un comité de supervisión de la Seguridad Informática, y el proceso para planificar y presupuestar la Seguridad Informática. Una vez definida la responsabilidad en materia de Seguridad Informática en las misiones departamentales y en las descripciones de cargos, el próximo paso es una evaluación del riesgo. Al completarse la estimación del riesgo, debe prepararse un documento inicial de políticas de Seguridad Informática. Otros documentos, tales como las normas y los procedimientos operativos, surgirán como subproductos del documento de política y de esfuerzos posteriores. Los temas relativos al cronograma necesario para la preparación de las políticas se discutirán en detalle más adelante, en la subsección titulada “[Cronograma para el Desarrollo de las Políticas](#)” en la página 22.

Orientación del Proceso de Selección y Desarrollo de Productos

La mayoría de las organizaciones no cuentan con los recursos necesarios para diseñar e implementar sus propios controles. Frecuentemente lo que hacen es seleccionar de un grupo de controles ofrecidos por los proveedores, y tratan de adaptarse con políticas, procedimientos, normas y otros esfuerzos de integración específicos de la organización. Este proceso de integración frecuentemente se realiza sin entender debidamente los objetivos de seguridad y las metas de la organización. Como resultado, los productos de seguridad seleccionados pueden no responder a sus verdaderas necesidades. Por ejemplo, la compra de dispositivos para fijar los computadores a las mesas pudo haber sido motivada por una ola de robos. En ausencia de políticas orientadoras, la gerencia puede haber seleccionado un producto que ni siquiera permite el almacenamiento fácil y seguro de los computadores portátiles.

Para evitar estos problemas, los objetivos y los requisitos de seguridad declarados en las políticas pueden proporcionar a los empleados tanto el entendimiento como la orientación adicional necesarios para actuar en concordancia con la gerencia. Tales políticas pueden ser una manera de garantizar que el personal interno debidamente selecciona, desarrolla e implementa los sistemas de información, porque son los autorizados. Por ejemplo, una política puede establecer el uso de aquel software antivirus autorizado por la gerencia de Seguridad Informática y ningún otro. El nombre del proveedor y el del producto pueden cambiar de mes a mes sin necesidad de cambiar la política. Esos detalles podrán aparecer en la norma, pero no en la política.

Demostración del Apoyo Gerencial

Algunas personas, particularmente los usuarios y personal del departamento de Tecnología de Información, frecuentemente dicen, "Cuando me digan algo, me ocupo de la Seguridad Informática". Esta actitud no es sorprendente cuando se aprecia en la mayoría de la gente una falta de conciencia sobre la magnitud de los riesgos que enfrentan en materia de Seguridad Informática, así como que tampoco tienen la disposición de tomarse un tiempo para analizar seriamente dichos riesgos. Aparte de esto, por no contar con la pericia requerida, la mayoría de las personas no puede estimar la necesidad de establecer ciertas medidas de control.

Por ello, las políticas representan la manera más definitiva que la gerencia puede utilizar para demostrar la importancia de la Seguridad Informática, y que los trabajadores tienen la obligación de prestar atención a la Seguridad Informática. Las políticas pueden compensar aquellas influencias que, de otra manera, evitarían que se prestara suficiente protección a los recursos informáticos. Un ejemplo frecuente es el de los gerentes de mediano nivel que, en repetidas ocasiones, se niegan a asignar recursos en sus presupuestos a la Seguridad Informática. En este caso, la otra influencia es el bono que frecuentemente reciben como recompensa por mantener los costos bajos. Pero los gerentes de mediano nivel no pueden seguir negando las solicitudes de fondos para la Seguridad Informática si el apoyo es exigido por la alta gerencia.

La gerencia en toda organización tiene que aclarar sus intenciones con respecto a la operación de los computadores y las redes. Si la gerencia dedica tiempo a preparar una política de seguridad informática y su correspondiente documentación, entonces al presentarse el momento que sea necesaria la acción disciplinaria, la demanda o la litigación, la organización no estará sujeta a estos mismos problemas legales. Las políticas además representan para la gerencia una manera relativamente barata y directa de definir el comportamiento correcto.

Cómo Evitar la Responsabilidad Legal

Aparte de los reglamentos al respecto, existe enorme evidencia de casos en los que la gerencia, e inclusive el personal técnico, puede tener responsabilidad legal por no atender adecuadamente los asuntos relativos a la seguridad informática. El fundamento de esta responsabilidad puede estar en la negligencia, la infracción del deber fiduciario, las fallas en el uso de las medidas de seguridad encontradas en otras organizaciones del mismo ramo, las fallas en el ejercicio del debido cuidado que se espera de un profesional de la computación, o la falta de actuación después de ocurrir una notificación real de que el sistema estará o está comprometido. Las discusiones sobre la exposición a la responsabilidad legal y la necesidad de establecer políticas son usadas con éxito muchas veces para atraer mayor atención y apoyo de la gerencia hacia los esfuerzos de Seguridad Informática. Se recomienda consultar con el departamento legal antes de presentar este tópico a la gerencia.

En los tribunales, las políticas han demostrado ser una evidencia influyente que manifiesta la preocupación de la gerencia sobre la Seguridad Informática y de las medidas tomadas al respecto. Si la organización aún no

ha tratado el tema de la Seguridad Informática, es importante iniciar pronto el trabajo y establecer de una vez la dirección de los esfuerzos futuros.

Protección de Secretos Industriales

Aunque las leyes referentes a los secretos industriales varían dependiendo de la jurisdicción, las políticas pueden proporcionar protección adicional para la propiedad intelectual delicada. En los tribunales, las políticas pueden servir como prueba para demostrar que

la organización ha adoptado medidas serias para proteger su propiedad intelectual, convenciendo así al tribunal de declarar una determinada propiedad intelectual como secreto industrial. Si la información es considerada secreto industrial, una organización tendría soluciones legales adicionales en las cuales fundamentar la exigencia de mayores compensaciones monetarias o de un amparo judicial. La [Tabla 2-1](#) incluye muchas razones para establecer políticas de Seguridad Informática dentro de la organización.

Tabla 2-1: Razones para Establecer las Políticas

Razón	Resultado
Aumentar el presupuesto de seguridad informática y agregar más personal.	El proceso de desarrollo de las políticas muestra a la gerencia lo que se requiere.
Establecer vía de comunicación con la alta gerencia.	La participación de la gerencia en el proceso de desarrollo abre nuevos canales.
Mostrar progreso definitivo con poca inversión.	Sólo se necesitan días o semanas para generar un documento creíble sobre las políticas.
Establecer la credibilidad y la visibilidad del esfuerzo realizado en la seguridad informática.	El documento sobre políticas debe ser refrendado con la firma del Jefe Oficial Ejecutivo de la empresa en la cubierta.
Cambiar las actitudes de los trabajadores y sus perspectivas.	Es crucial el apoyo de todos los trabajadores que interactúan con los sistemas informáticos.
Armonizar y coordinar las actividades de muchos trabajadores.	Para mantener la seguridad se requieren medidas constantes.
Definir los límites de las acciones que se pueden permitir.	Los trabajadores entenderán los límites de sus responsabilidades asignadas.
Controlar con anticipación los eventos relativos a la seguridad.	Aumenta la probabilidad de que las cosas se harán de manera correcta la primera vez y disminuye los errores.
Ejercer control mediante la excepción en lugar de la microgerencia.	No es necesario revisar cada medida y cada decisión.
Superar la ambigüedad que pueda dar origen a la sobrecarga informática.	Un documento sobre políticas enfocará la atención del trabajador en lo esencial.
Permitir que la gerencia determine si el trabajador ejerció buen o mal juicio.	No existen medidas disciplinarias si se ejerció mal juicio.
Evitar disputas y otras querellas internas.	El reglamento a seguir y los límites estarán definidos en las políticas.
Facilitar el rápido desarrollo de nuevos sistemas.	Los requerimientos estarán definidos previamente, así que no habrá necesidad de revisarlos.
Coordinar actividades de grupos internos y externos.	Las políticas permitirán el establecimiento de una extranet o el uso de una organización tercera.
Lograr costos más bajos mediante la normalización de los controles.	El mismo enfoque puede utilizarse uniformemente a lo largo de la organización.
Evitar problemas porque las tareas se encuentran fuera de secuencia.	En asuntos cruciales, no se requerirá que el personal adivine los pasos siguientes que proceden.

Tabla 2-1: Razones para Establecer las Políticas (Continued)

Razón	Resultado
Evitar que los grupos descentralizados “reinventen la rueda”.	Si se especifican las políticas de manera centralizada, los grupos locales no necesitan desarrollarlas.
Establecer un punto de partida de un proceso de mejoramiento continuo.	Las políticas representan la línea de base a la cual todos se pueden referir y sobre la cual se construye el mejoramiento.
Demostrar procesos de control de la calidad.	Para el cumplimiento de ISO 9000 se exige que las reglas del negocio estén claramente documentadas.
Establecer puntos de comparación y de referencia para auditorías futuras.	Los auditores internos pueden determinar si existe cumplimiento.
Orientar la implementación, así como la selección del servicio y del producto de seguridad.	Reduce las posibilidades de que los grupos locales no coordinados busquen sus propias soluciones.
Garantizar la consistente implantación de los controles.	Cada excepción debilita el control correspondiente, pero con la política se exige el cumplimiento del control.
Recaudar las obligaciones contractuales para proseguir casos en tribunales.	La utilización de los acuerdos de cumplimiento de políticas y de confidencialidad.

Adaptación a un Ambiente Comunicacional Dinámico

Los trabajadores de las organizaciones muestran señales crecientes de fatiga y de recarga de información. La proliferación de nuevas tecnologías comunicacionales, como los computadores, Internet, las máquinas facsimiles, las fotocopiadoras y los buscapersonas, ha desestabilizado los antiguos procesos comunicacionales. Por ejemplo, antes se consideraba de buen gusto devolver una llamada telefónica, pero ahora no si el que pide la devolución de la llamada es un vendedor. La falta de reglas claras que dicten la conducta apropiada en este ambiente tan dinámico ha dificultado la vida de los trabajadores. Por ello, a fin de manejar eficazmente las expectativas de los trabajadores y ayudar a orientar su conducta, la gerencia debe eliminar esta molesta ambigüedad mediante el establecimiento de prioridades claras y la definición de acciones apropiadas. Los mensajes contenidos en este manual tienen justamente ese fin, pero en el ámbito de la seguridad informática.

Logro de Seguridad Completa y Consistente

Uno de los problemas más graves del campo de la seguridad informática tiene que ver con los esfuerzos fragmentados e inconsistentes que al respecto abundan.

Demasiadas veces un departamento estará feliz de prestar su colaboración en materia de seguridad informática, mientras que otro de la misma organización se mostrará reacio. Dependiendo de los recursos computacionales que comparten estos departamentos, como la intranet, el departamento reacio crea peligros informáticos para el otro departamento. Esto podría suceder, por ejemplo, si un hacker obtuviera acceso a la intranet a través de un descuidado proceso de autentificación de usuario dentro del departamento reacio, y luego utilizara esta invasión para destruir información del departamento que sí presta atención a su seguridad. Aunque no es ni posible ni deseable que todas las personas de la organización estén familiarizadas con las complejidades de la seguridad informática, sí es importante que todos se suscriban a un nivel mínimo de protección. En términos de alto nivel, las políticas se utilizan para definir dicho nivel mínimo de protección, que algunos llaman línea de base.

Coordinación de las Actividades de los Grupos Internos y Externos

Utilizar terceros, contratistas, consultores y personal temporal ya se ha convertido en una necesidad de las organizaciones, que a su vez deben establecer nexos empresariales cercanos con otras organizaciones,

incluso cuando éstas representan competencia.. La enorme cantidad de entes empresariales existentes ha dificultado el manejo de cosas como el control del acceso, la protección de la propiedad intelectual y todo lo relativo a la seguridad informática. Debido a que tanta gente está involucrada, existe la necesidad apremiante de coordinar consistentemente las actividades de los grupos internos y externos. Y allí es exactamente donde las políticas de seguridad informática pueden prestar gran ayuda. Por ejemplo, una política puede definir cuándo y dónde se requiere la firma de un acuerdo de confidencialidad, e igualmente definir cuándo no. Así que el gerente que esté a punto de contratar a alguien simplemente se lee la política correspondiente, soluciona el problema y protege los activos informáticos. Todo de una sola vez.

Históricamente la información sensible siempre estuvo en las manos de la media y alta gerencia. Pero ahora es empujada hacia la parte inferior de la jerarquía, hacia los

computadores de los empleados y hacia afuera, a contratistas, consultores y temporales. A medida que más gente se involucra en el área de seguridad informática, y a medida que más gente tiene acceso a información confidencial, crítica o valiosa, más necesarias se hacen las políticas de seguridad informática.

Supervisar directamente a toda esta gente no es práctico, y las herramientas tecnológicas con buena relación precio-valor para hacerlo no están disponibles todavía. Aunque las organizaciones rara vez lo admitan, toda esta gente necesita aprender a auto-gestionarse, pero necesitan las instrucciones adecuadas para poder hacerlo bien. Lo mejor en seguridad informática tiene que ver con la confianza no supervisada en la gente, porque herramientas sofisticadas no hay, por lo menos todavía. Así que la herramienta Nº 1 para el manejo de la conducta de la gente en el área de seguridad informática lo constituye el documento de políticas de seguridad informática.

Pasos para el Desarrollo de las Políticas

Recopilación de Materiales de Referencia Clave

Las políticas de Seguridad Informática deberían ser impulsadas en su mayoría de acuerdo con la naturaleza de la información manejada por la organización. Todos deberíamos familiarizarnos con ella. Una buena fuente de esta información es un diccionario de datos, también conocido como metadata. Otros antecedentes útiles para el desarrollo de políticas los contituyen los bosquejos de sistemas informáticos internos preparados para altos ejecutivos, integrantes de juntas directivas, empresas listas para fusiones y adquisiciones y para socios estratégicos. Debido a los rápidos cambios en los sistemas informáticos, es probable que la documentación disponible ya esté obsoleta. También se puede entrevistar a trabajadores expertos para identificar con precisión la naturaleza de la información manejada en la actualidad, incluyendo cuál parte de ella es confidencial, cuál es valiosa y cuál es crítica.

Al elaborar un conjunto de políticas de Seguridad Informática, se debería revisar la última evaluación de riesgo o auditoría informática que refleje claramente las necesidades actuales de seguridad informática de la organización. Un historial de pérdidas que documente los detalles de incidentes recientes también puede ser de ayuda en identificar áreas en necesidad de mayor atención. Las demandas judiciales, los reclamos formales escritos y otras disputas pueden identificar

áreas que merezcan atención en el documento de política. Para identificar otras áreas con problemas, se recomiendan reuniones con el consultor jurídico de la organización, el director de Seguridad Física, el jefe oficial de Información, el director de Auditoría Interna y el director de Recursos Humanos.

Para identificar otras áreas en necesidad de mayor atención, se deben reunir copias de otros documentos organizacionales relevantes y actuales de política. Las políticas relevantes incluyen las políticas de desarrollo de sistemas de aplicaciones, las políticas de operaciones computacionales, las políticas de adquisición de equipos de computación, las políticas de recursos humanos, las políticas de control de calidad del sistema informático y las políticas de seguridad física. Si se pueden obtener, las políticas de otras organizaciones en el mismo ramo proporcionarían información útil sobre los antecedentes. Si la organización es una subsidiaria o está afiliada a otra organización, entonces se debe acudir a la casa matriz para obtener información y la misma debe ser usada como referencia. Si la organización participa en una red electrónica de intercambio de datos, o en cualquier otra, se deben obtener y revisar las políticas de dichas redes.

Algunos de los que enfrentan limitaciones significativas de tiempo o de recursos se sentirán tentados a ignorar el proceso de recopilación de antecedentes y datos aquí mencionado. Si se abrevia significativamente la recolec-

ción de datos, aumenta la probabilidad de rechazo del documento resultante por parte de la gerencia. Es gracias a este proceso de recolección de datos que se pueden identificar la visión de la gerencia sobre la Seguridad Informática, las políticas ya existentes, las políticas que necesitan añadirse o cambiarse, la manera en que la gerencia logra el cumplimiento de las políticas, las vulnerabilidades particulares de la organización y demás información histórica esencial. Si no se da la consideración adecuada a esta información histórica, es poco probable que la política de Seguridad Informática resultante pueda responder a las verdaderas necesidades de la organización.

Otra razón importante para hacer numerosas investigaciones de los antecedentes es para preparar la política de manera de garantizar que los requisitos definidos en el documento de política coinciden con las intenciones de la gerencia. Una de las formas mas rápidas de perder credibilidad al momento de redactar una política de Seguridad Informática es la de proponer una política claramente inconsistente con las normas de la organización. Por ejemplo, los empleados de una firma de alta tecnología en forma rutinaria bajaban juegos de Internet y los jugaban en sus poderosos terminales durante los recesos y las horas no hábiles. La alta gerencia tenía conocimiento de esto y tácitamente lo aprobaba. Al mismo tiempo, una política publicada indicaba que no se toleraría ningún uso personal de los sistemas de la empresa. Esta grotesca inconsistencia hizo que la gran mayoría de los trabajadores de esta empresa descartara, por irrelevante, el documento de política.

Otra razón importante para dedicarle tiempo a la investigación de antecedentes es la de definir las direcciones estratégicas de la organización en relación con los negocios. Un documento nuevo o revisado necesita ser consistente con estas direcciones estratégicas si la alta gerencia ha de aprobar y apoyar la política. Por ejemplo, supongamos que una organización desea centralizar nuevamente sus actividades de sistemas de información ahora descentralizadas. Un documento de política que resalte muchas actividades descentralizadas a ser realizadas por un grupo de coordinadores de Seguridad Informática sería inconsistente con las intenciones de la gerencia y, lógicamente, no sería probable la aprobación del documento.

Existe todavía otra razón más para efectuar una investigación completa de la situación actual al comenzar el proceso de redacción. Se trata de la identificación de la arquitectura de los sistemas informáticos internos, ya que el documento debería ser consistente y apoyar totalmente la arquitectura de los sistemas informáticos existentes. Es decir, no se trata de atender la arquitectura de la Seguridad Informática sino la arquitectura de los sistemas informáticos. El documento de política de Seguridad Informática comúnmente se desarrolla cuando ya existe la arquitectura de sistemas informáticos. El desarrollo de un documento de políticas de Seguridad Informática permitirá la elaboración de una arquitectura de Seguridad Informática. Por ejemplo, una política sobre el acceso permisible a través de un cortafuego de Internet posibilitará la determinación de la arquitectura de seguridad y también posibilitará la selección e incorporación del cortafuego adecuado.

Definición de un Marco de Referencia para las Políticas

Después de reunir los materiales de referencia antes mencionados, debe recopilarse una lista contentiva de los tópicos a cubrir en un documento de políticas de Seguridad Informática nuevo o de mayor alcance. El primer borrador de la lista debe incluir políticas destinadas a la adopción inmediata y aquellas destinadas a la adopción futura. En la mayoría de los casos, el nivel de detalle en esta lista será inconsistente y, en esta etapa del proceso, no debería causar preocupación. Por ejemplo, la lista puede incluir el teletrabajo y la construcción de contraseñas con un mínimo de 10 caracteres. Al estar listo el esquema de alto nivel, el nivel de detalle debería normalizarse. Para mayor información, ver “[Preparación de una Matriz de Cobertura](#).”

El próximo paso a seguir es el intento de definir las formas en las que la organización se propone expresar las políticas de Seguridad Informática. Por ejemplo, las políticas pueden colocarse en un manual de procedimientos operativos. Como alternativa, el director del departamento de Seguridad Informática periódicamente puede emitir memorandos por correo electrónico resumiendo las políticas. Es común colocar las políticas de privacidad en Internet. Debido a que los trabajadores son sometidos constantemente a comunicaciones de muchas personas a través de múltiples canales, es importante enviar repetidamente a través de dichos canales las políticas de Seguridad Informática. Para mayor información sobre las sugerencias de las formas de comunicar las políticas, ver Apéndice D, “[Lista de Métodos Sugeridos para Aumentar Nivel de Conciencia](#). ” Los canales usados para expresar una política determinarán como debe estar redactada. Por ejemplo, si se usa una cinta de video, entonces debe emplearse un estilo coloquial abreviado. Si un documento de política permanece en un servidor de Intranet, entonces un estilo más gráfico y con hipertextos es el apropiado.

Deben examinarse las formas en que una organización en la actualidad usa y se propone usar las políticas de Seguridad Informática. Las políticas pueden usarse para guiar los esfuerzos de adquisición de sistemas informáticos, impulsar los planes de auditoría de la tecnología informática y ayudar a los usuarios a operar con seguridad sus computadores. Para más ideas sobre usos potenciales, ver [Tabla 2-1 “Razones para Establecer las Políticas”](#). Definir los usos de las políticas identificará las audiencias a quienes deben ser dirigidas las políticas.

Para obtener información adicional sobre la identificación de públicos, ver “[Preparación de una Matriz de Cobertura](#).”

Determinar los usos de las políticas también concentrará la atención en aquellas áreas con mayor necesidad. Otros usos se harán mas aparentes después de distribuir el documento de política, lo cual no debe verse como falta de planificación sino como una exitosa iniciativa que posee contribuciones futuras para la organización. En algunos casos, los usos de un documento de política serán desconocidos al principio, pero ya se podrán determinar mediante una serie de reuniones con los interesados.

También debe estudiarse el estilo utilizado para la redacción de las políticas, el uso de ciertas palabras, el formato convencional para documentar las políticas, el sistema utilizado para numerar y dar nombre a las políticas, y los enlaces entre las políticas y otras directrices gerenciales, tales como los procedimientos y las normas. Por ejemplo, las políticas existentes pueden utilizar el verbo “deber”. Para mantener la consistencia, las políticas de seguridad informática también deberían usar el mismo verbo. Igualmente, las políticas actuales podrían tener un sistema de numeración estilo militar o algo completamente diferente. La emisión de un documento de políticas de seguridad informática es controversial por naturaleza, así que no dé motivos a sus detractores y mantenga la consistencia necesaria con los lineamientos de estilo, estén dichos lineamientos escritos o no.

Parte del estudio de las políticas existentes y cómo se utilizan debería incluir también una revisión del nivel de detalle apropiado para el enunciado específico de las políticas. La organización puede haber definido las políticas existentes en palabras muy específicas, en cuyo caso muchas políticas muy detalladas sería lo adecuado. Por otro lado, las pudo haber definido en términos de muy alto nivel, en cuyo caso sólo una breve declaración generalizada sería suficiente. Ambas alternativas pueden coexistir por el hecho de que las distintas políticas están dirigidas a distintos públicos. El nivel de detalle es en parte impulsado por el nivel de confianza que la gerencia tiene en la habilidad de sus trabajadores para tomar las decisiones apropiadas, el nivel de cumplimiento observado de los requisitos específicos y el nivel de novedad que tienen los tópicos para el público al cual se dirigen.

Poca información documentada existe sobre la expresión, el uso, el estilo y nivel de detalle de las políticas internas, pero puede obtenerse examinando los enunciados de políticas existentes. En algunas organiza-

ciones grandes puede existir un documento que ofrezca directrices sobre el proceso de redacción de políticas. En otras, existen grupos de Planificación y Políticas que pueden prestar ayuda en este proceso de redacción. Sin importar cuál esté disponible, y para garantizar su rápida adopción por parte de los interesados, toda política nueva o modificada relativa a la seguridad informática debe estar redactada de manera igual, o por lo menos parecida en su forma, a las políticas actuales.

Preparación de una Matriz de Cobertura

Se recomienda usar las políticas de este manual después de preparar un borrador de las áreas que necesitan atención, y después de familiarizarse con las maneras cómo las organizaciones expresan y utilizan sus propias políticas. En este punto es conveniente evaluar los tópicos adicionales a cubrir. Revise los títulos de las políticas o las políticas mismas, pero no lea los comentarios correspondientes. Esta tarea se completa más rápidamente con una copia en papel y marcador, tal como un resaltador amarillo.

Para obtener más ideas para las áreas a cubrir, puede utilizar la Tabla de Contenido de este manual. Pero, aunque esta Tabla es útil y proporciona buena cobertura de los tópicos principales, deben desarrollarse categorías que respondan a las necesidades específicas de cada organización. Por otro lado, las categorías que reflejan las áreas a cubrir también pueden seguir el patrón de un informe interno de auditoría o el de una guía de seguridad informática con algún valor para la gerencia. Otra manera de segmentar los controles estarían representados por los objetivos, tales como “evitar”, “prevenir”, “detener”, “detectar”, “mitigar”, “recuperar” y “corregir”.

En este punto debería desarrollarse el borrador de un esquema de alto nivel que refleje los tópicos a tratar. Este esquema queda mejor si viene acompañado de una breve explicación con ejemplos de los tópicos que debe cubrir cada sección. La explicación puede ser de sólo una oración o dos o justo lo suficiente como para proporcionar un bosquejo de los tópicos incluidos. Ahora se recomienda la distribución del esquema a las partes interesadas y, luego, la crítica constructiva que se reciba debe integrarse al esquema de alto nivel ya mencionado.

Ahora se debe determinar cuáles serán las audiencias a las cuales se dirigirán estos mensajes. A menudo las políticas deben estar dirigidas a audiencias muy diferentes porque cada una de ellas tiene necesidades muy diferentes. Por ejemplo, los usuarios finales pueden recibir un pequeño folleto que contiene las políticas de

seguridad informática más importantes que ellos deben recordar y su énfasis podría estar en los problemas de seguridad informática de los computadores personales. Al mismo tiempo, los desarrolladores de sistemas y otros técnicos podrían recibir un documento mucho más largo y con mucho más detalle, quizás enfatizando la seguridad como una parte de la metodología normal de desarrollo de sistemas. La gerencia, por su parte, recibiría otro documento relacionado principalmente con las tareas de los Propietarios de la información.

Si bien parece mucho esfuerzo producir documentos separados para distintos públicos, el trabajo adicional en realidad no es gran cosa si se ha preparado una lista de los mensajes esenciales que deben comunicarse. Esta lista ahora se puede dividir de acuerdo con el tipo de audiencia, y ése es el proceso que se discute en los próximos párrafos. El desarrollo y mantenimiento de documentos separados para distintas audiencias se facilitan si se colocan en una intranet. Usando enlaces a través de un navegador, los que lean la política pueden rápidamente recibir sólo la información que es importante para ellos. Por ejemplo, una intranet se usa en un banco para segmentar las políticas de seguridad informática de acuerdo con el cargo del empleado, así que cada uno sólo lee las políticas que le corresponden. La intranet también ofrece un mecanismo de búsqueda y un índice, los cuales ayudan a los lectores a rápidamente encontrar las políticas que les interesan. Las intranets también pueden ser utilizadas para administrar exámenes cortos para garantizar el entendimiento de las políticas.

Cuando ha de dirigirse a más de dos públicos a través de documentos separados, se recomienda la preparación de una “matriz de cobertura” antes de redactar el primer borrador de las políticas. Esto se puede lograr preparando un esquema detallado separado para cada una de las audiencias. Una matriz de cobertura es sólo una herramienta organizacional que garantiza que todos los mensajes de seguridad informática se presentan a las audiencias correspondientes. Es una manera de ver el trabajo a realizar, prestando algún tipo de orden a lo que de otra manera resultaría un complicado esfuerzo de redacción. Una vez identificados los tópicos a comunicar, y organizados en una matriz de cobertura, la preparación en sí de los documentos de las políticas será relativamente fácil.

En su forma más sencilla, una matriz de cobertura no es más que una tabla de dos dimensiones. Puede, por ejemplo, utilizar las audiencias primarias a quienes están dirigidas las políticas como los títulos de las filas, y las categorías de políticas como los títulos de las columnas. Estas categorías son las secciones principales

que aparecen en el esquema de alto nivel ya mencionado. Las celdas del centro de la matriz deben llenarse con números de referencia, donde cada uno se refiere a una política del manual y quizás a otra parte.

Dado que probablemente habrá muchas columnas y pocas filas, se recomienda una matriz de cobertura tipo plantilla con los títulos de fila para las audiencias, los títulos de columna en blanco para las categorías de políticas y celdas en blanco en el medio para las políticas específicas. Esta plantilla de matriz puede ser entonces fotocopiada varias veces para ahorrar mucho tiempo en la creación de otras matrices de cobertura. Si no es problema ver sólo una parte de la matriz a la vez, se ahorra más tiempo si se utiliza un programa de hoja de cálculo para construir y manipular la matriz. Utilizar la hoja de cálculo también produce mejores copias y facilita la actualización de la matriz.

A menudo sólo se necesitarán dos o tres audiencias. Dos audiencias posibles pueden ser los usuarios finales y el personal técnico de los computadores. Bajo otro enfoque, podríamos tener tres: usuarios finales, la gerencia y el soporte técnico. En casi cualquier instancia, habrá semejanzas en los mensajes dirigidos a cada una de estas tres audiencias. Haga todos los esfuerzos por minimizar la cantidad de audiencias, pero reconociendo la necesidad de cada grupo de recibir información diferente.

La [Tabla 2-2](#) proporciona un ejemplo del tipo de matriz que se puede desarrollar. Los números de las políticas que aparecen en la matriz son para conservar los lugares y, deliberadamente, no provienen de un análisis. Cada organización necesitará preparar su propia matriz de cobertura e insertar los números de las políticas donde correspondan con el fin de reflejar su propio y único ambiente empresarial e informático.

Si desarrollar este tipo de matriz de cobertura parece tomar demasiado tiempo, se puede preparar una tabla similar con categorías amplias, tales como las mostradas en la Tabla de Contenido de este manual.

Un enfoque alternativo proporciona lo que podría considerarse un balance entre una sola política y varias políticas para diferentes audiencias. En este caso, un documento de políticas tipo paraguas puede aplicarse a todo el personal, y se pueden utilizar documentos especializados para atender a los Propietarios de la información, los desarrolladores de sistemas, los que realizan teletrabajo y otras audiencias específicas. Este enfoque permite aplicar un conjunto básico de reglas a todos, y también políticas especiales para audiencias específicas. Este enfoque está siendo cada vez más utilizado en organizaciones grandes que cuentan con intranets.

Tabla 2-2: Modelo de Matriz de Cobertura

Audiencia	Computadores	Comunicación de Datos	Gestión de Riesgo	Seguridad Física
Usuarios Finales	9.03.01.08 9.03.01.09 9.05.04.13 9.06.01.02	9.02.03.11 9.03.01.09 9.03.01.10 9.03.01.11 9.03.01.12 9.04.03.03 9.05.04.13 9.06.01.02	5.02.01.02 5.02.01.03 8.07.06.31	9.05.04.13 9.05.04.22 9.06.01.02 10.03.02.11
Gerencia	9.04.07.01 9.05.04.13 9.05.04.22 12.01.03.02 12.01.04.23	12.01.04.04 12.01.04.87 12.01.04.88 12.01.04.89 12.01.05.16 12.01.07.03	9.03.01.08 9.03.01.10 9.03.01.11 9.03.01.12 9.02.03.09 9.02.03.10 9.02.03.12 9.04.03.04	8.04.01.15 8.07.05.47 8.07.05.48 9.03.01.07 9.03.01.08 9.04.07.01 9.05.04.22 9.05.05.06 9.05.05.07 9.05.06.01 9.06.01.02 10.04.02.02 12.02.02.01
Departamento de Sistemas Informáticos	9.04.03.04 9.05.03.03 9.05.04.22	8.03.01.15 10.02.02.02 10.02.02.03	6.03.01.04 8.06.01.01 8.06.03.06	8.01.02.01 8.03.01.19 9.02.01.01 9.05.04.08 9.05.04.13 9.05.04.17 9.07.02.16 10.02.02.05 10.05.01.07 10.05.01.08 10.05.01.09 10.05.01.10 12.01.04.20
Clientes	8.03.01.20 8.03.01.21 10.05.01.14	10.01.01.06 10.01.01.07 10.05.01.04	9.05.03.03 9.05.04.22 9.05.04.23 9.05.06.01	9.05.03.03 9.05.04.23 9.05.06.01 9.06.01.02
Socios Comerciales	8.02.02.07 8.02.02.08 8.02.02.09	5.02.02.04 10.01.01.08 10.01.01.09	9.03.01.04 9.03.01.05 9.03.01.06 9.05.04.24	8.07.06.09 9.05.02.01 12.01.04.32 12.01.04.42 12.03.01.01

Con la intención de ahorrar tiempo, algunas personas a menudo suponen que habrá sólo una audiencia. Este enfoque “talla única” puede servir para las primeras pocas políticas emitidas por una organización, pero mientras más sofisticado sea el esfuerzo en seguridad informática, menos se adaptará a este enfoque. Se ahorrará considerable tiempo si las distintas audiencias se convierten en objetivo desde el principio de la redacción de la política en lugar de tener que modificar la talla única, cuya intención original era satisfacer las necesidades de múltiples audiencias. Las distintas audiencias también agradecerán la utilización de documentos separados. Si se utilizan documentos separados, no habrá necesidad de avisar a cada audiencia que ha habido cambios en las políticas que, en muchos casos, no les afectarán. Además, utilizar

documentos separados permitirá un tratamiento diferencial sin crear confusión. Por ejemplo, el reglamento para permitir el acceso de terceras personas a los sistemas informáticos de la organización puede ser muy diferente del que permite el acceso a los empleados permanentes.

El que existan distintas audiencias para las políticas no quiere decir necesariamente que tiene que haber distintos documentos. Es posible tener diferentes capítulos o secciones en un manual de seguridad informática dirigido a distintas audiencias. Este enfoque resulta atractivo porque todas las políticas se encuentran entonces en un solo documento en lugar de varios. Un solo manual también facilita el mantenimiento y las revisiones. Los individuos a menudo se encuentran en dos o más audiencias. Por ejemplo, alguien puede ser a la vez un usuario general y un desarrollador de sistemas.

Ahora deben escribirse los números de las políticas directamente en el cuerpo de la matriz de cobertura. El proceso de llenar el cuerpo de la matriz a menudo resalta el hecho de que ciertas audiencias no están siendo tomadas en cuenta apropiadamente, así como a menudo indica que ciertas áreas requieren de políticas adicionales para realmente poder responder a las necesidades de la organización. Si se hubiera preparado el esquema del documento de políticas para distintas audiencias, pero no la matriz, estas discrepancias quizá no se habrían notado.

Si un área no está adecuadamente atendida, los índices de este manual así como la Tabla de Contenido pueden ser referenciados para obtener ideas adicionales. El CD-ROM de este manual puede hacer búsquedas por palabras clave. Por ejemplo, si se necesitan políticas antivirus adicionales, la búsqueda con la palabra “virus” brindaría rápidos resultados.

Después de aclarar los tópicos generales en la matriz de cobertura, se puede compilar un esquema detallado de los documentos de las políticas. Dependiendo de la gerencia, puede haber necesidad de lograr que las partes revisen el esquema detallado. Si no se requiere tal revisión, entonces no hará falta. En ese caso, se puede empezar a redactar el documento de políticas utilizando la matriz de cobertura.

Si se nota un alto nivel de incertidumbre política en el proceso de redacción del documento, podría prepararse un esquema detallado y someterlo a un proceso de revisión. Si bien esto puede demorar el proceso, garantiza que el documento resultante cubrirá el objetivo deseado y responderá de verdad a las necesidades de la organización. Si el documento está dirigido a una sola audiencia, se puede eliminar la matriz de cobertura, pero sí debe prepararse un esquema detallado. Cualquiera de los dos es importante. Sin uno o el otro se pueden perder semanas completas redactando políticas sobre tópicos no necesarios o no deseados por la gerencia.

En este punto debe tomarse la decisión de cuáles categorías se utilizarán en el documento de políticas. Las categorías de la matriz de cobertura o del esquema deberían ser suficientes, aunque a menudo serán modificadas durante el período de revisión. Se recomienda un gran número de subtítulos, porque ayuda a los lectores a localizar con rapidez los tópicos de interés. Así no tienen que leer las secciones que no les corresponden.

Si se está desarrollando un documento de políticas muy extenso, o si contiene grandes complejidades, puede utilizarse un mapa mental. Los mapas mentales son

representaciones gráficas de las relaciones que existen entre las ideas, generalmente utilizando círculos para representar las ideas y flechas para representar la relación entre ellas. Un mapa mental puede convertirse rápidamente en un complejo esquema que puede utilizarse para desarrollar un borrador de un documento de políticas. Existen en el mercado varios programas de software y guías que pueden ayudar a dibujar y revisar mapas mentales.

Después de terminado el proceso de redacción, la matriz de cobertura, los esquemas y demás papeles de trabajo deben ser almacenados. Probablemente se necesitará revisar el documento en un par de años y la persona encargada de hacer la revisión se ahorrará mucho tiempo si puede consultar los papeles originales. La matriz de cobertura y los demás papeles también pueden servir en los tribunales en caso de que alguien sugiera que la gerencia no tomó en cuenta los verdaderos riesgos y los mensajes de política que tenían que haber sido comunicados en su momento.

Igualmente, los papeles de trabajo deben retenerse por un período de un año a dos porque los auditores internos o externos pueden desear verlos. Tener los documentos de trabajo bien resguardados en un sitio accesible también puede ser importante en caso de que algún integrante de la gerencia reclame que sus comentarios nunca fueron integrados al documento final .

Toma de Decisiones Críticas en el Diseño de Sistemas

Antes de publicar la versión final del documento de políticas, la gerencia a menudo necesita tomar una serie de decisiones relativas a la seguridad en el diseño de los sistemas. Algunos ejemplos son los siguientes:

- Grupos de Usuarios que recibirán acceso a Internet.
- Frecuencia para dicho acceso, si será continuo, regular u ocasional.
- Tipo de acceso que necesitarán: correo electrónico, navegación en la web, transferencias de archivos, accesos remotos o salones de chat.
- Tipo de control de acceso: contraseñas dinámicas, fijas o tarjetas inteligentes.
- Tipos de actividad del usuario que será monitoreada: archivos transferidos, sitios web visitados o uso de horas por día.

La identificación de estas y otras decisiones en el diseño de los sistemas normalmente se logra de manera indirecta, porque típicamente se prepara un borrador del

documento que incorpora las opciones sugeridas. Desafortunadamente, con el fin de acelerar el proceso de redacción, las soluciones alternativas no se resaltan. Como resultado, la gerencia puede aprobar un documento de políticas que incorpore decisiones con implicaciones ulteriores que no se notan al momento de la aprobación. Esto puede resultar costoso para la seguridad informática, ya que los propuestas iniciales descritas en el documento pronto necesitarán reemplazarse o revisarse. También puede significar que el documento completo deba cambiarse mucho antes de lo que debería.

Si el cronograma del proyecto y los recursos lo permiten, deberían resaltarse las decisiones fundamentales en el diseño de los sistemas. Si se va a circular un borrador en papel de las políticas para recibir comentarios al respecto, debería llevar notas al pie que describan las opciones y sus ventajas y desventajas. Algunas palabras que reflejen las decisiones de diseño pueden ser incorporadas al cuerpo del borrador. Si ve las opciones en contexto, la gerencia tomará las decisiones con mayor facilidad. Si el borrador de la política se va a colocar en la intranet con acceso limitado a ciertas personas, ciertas palabras pueden resaltarse y utilizarse enlaces para iluminar las opciones y las justificaciones correspondientes.

En aquellas organizaciones que han estado prestando atención a la seguridad informática durante cierto tiempo, la gerencia ya habrá considerado seriamente todas las opciones fundamentales de diseño de sistemas. En estos casos, el esfuerzo de redactar la política simplemente significará documentar las decisiones ya tomadas y seleccionar vías apropiadas para expresar estas decisiones en forma de política. En estos casos, no habrá necesidad de realizar una revisión separada de los asuntos críticos del diseño de sistemas, tal como se menciona más arriba. Por el contrario, el enfoque puede residir en extender estas decisiones sobre diseños ya existentes a nuevos sistemas informáticos, tales como las extranets, y a nuevas tecnologías, tales como nuevos lenguajes de programación.

Estructuración de los Procesos de Revisión, Aprobación y Cumplimiento

Cuando se haya redactado el primer borrador del documento de las políticas de seguridad informática, debería ser revisado por varios colegas. Después de los cambios solicitados por dichos colegas, el documento de políticas debería ser enviado a las partes internas interesadas, tales como la gerencia de Auditoría Interna y al consejero legal para que revise lo relativo a la Propiedad Intelectual. Luego de que varios aliados cruciales hayan realizado sus cambios, estará listo el borrador para que lo revise el comité gerencial de Seguridad Informática. La siguiente versión del borrador puede enviarse a muchas otras personas, por ejemplo a todos los Propietarios de información y a todos los que trabajan en Sistemas Informáticos. Este proceso de revisión es aconsejable porque crea el respaldo necesario por parte de actores cruciales, pre-vendiendo el documento a estos actores cruciales y construyendo apoyo de los mismos actores cruciales.

Muchos ciclos de revisión, cada uno de ellos con más cambios al documento de políticas, usualmente son necesarios. Esto debe verse como procedimiento normal y no debe considerarse, desde ningún punto de vista, como un insulto personal. Las revisiones múltiples son en parte una reflexión del hecho de que el proceso de desarrollo de las políticas de seguridad informática es altamente político, emocional y altamente no estructurado. Toda opinión debe ser bienvenida con el agradecimiento de que este proceso de revisión tan reiterativo logra políticas más claras, concisas y que verdaderamente responden a las condiciones existentes en el entorno. Este manual contiene dos apéndices que proporcionan información adicional al respecto. Para mayor información, ver Apéndice G, “[Vista General de las Tareas del Proceso de Desarrollo de las Políticas](#)” y Apéndice F, “[Lista de Verificación de Pasos en Proceso de Desarrollo de Políticas](#).“

El paso final del proceso de revisión es la firma del gerente general, presidente, jefe ejecutivo o presidente de la junta directiva. Un breve mensaje que indique que el cumplimiento es requisito para continuar en el empleo debe estar en la primera página del documento de políticas o en la página web de apertura si la política es publicada en un servidor de la intranet. Este mensaje debe estar firmado por el alto ejecutivo en un sitio rápidamente visible de tal manera que el lector no acoja dudas de que el documento tiene el pleno apoyo de la alta gerencia. Si no hay posibilidad real de lograr la firma del presidente de la junta directiva, entonces la del jefe oficial de información debería ser suficiente. Pero nunca debe aceptarse sólo la firma de un gerente medio, mientras que la firma de la gerencia de Seguridad Informática no muestra suficiente apoyo y adopción por parte de la alta gerencia. Si bien obtener la firma de la alta gerencia suena como excesivo mercadeo, la experiencia ha demostrado que la firma del ejecutivo más importante y su mensaje acerca del cumplimiento es crucial para que se adopte en toda la organización. Antes de que la gerencia apruebe un documento de políticas, éste debe haber sido revisado y editado varias veces por las distintas personas de la organización. Quizás el cuerpo más adecuado para la revisión es un comité de gestión de la seguridad informática.

Un comité de gestión de la seguridad informática está generalmente compuesto por representantes de los departamentos de la organización interesados en la seguridad informática. Los participantes incluyen a integrantes de los departamentos de Seguridad Informática, Auditoría Interna, Gestión de Riesgos, Seguridad Física, Sistemas Informáticos, Recursos Humanos, Legal, Finanzas y Contabilidad, y varios departamentos usuarios. Tal comité usualmente supervisa el trabajo del departamento de Seguridad Informática. Este comité de gestión se utiliza para filtrar y refinar las políticas propuestas, los procedimientos, las estructuras organizacionales y otras iniciativas, de manera que puedan ser rápidamente adoptadas e implementadas a lo largo de la organización. En la mayoría de los casos, la gerencia de Seguridad Informática redactará un borrador de la política correspondiente y la presentará a la consideración del comité de gestión. Si la organización todavía no tiene un comité de gestión, el momento del desarrollo de una política de seguridad informática es el mejor para proponer entonces su creación. El comité está usualmente compuesto por cinco a ocho individuos experimentados en el área, y que se ven a sí mismos como influyentes en el campo de la seguridad informática y que pueden representar a sus propios departamentos o sus áreas de conocimiento. Para mayor información sobre este comité, ver *Responsabilidades y*

Roles en Seguridad Informática. La política denominada “[Comité de Gestión de Seguridad Informática](#)” también puede proporcionar orientación adecuada.

En algunos casos se forma un comité de desarrollo de las políticas de seguridad informática, sin importar si ya existe un comité de gestión de la seguridad informática. Este comité de desarrollo puede ser un subcomité del de gestión, pero no debe encargarse de la redacción de las políticas, porque frecuentemente las políticas redactadas por los comités son una combinación de ideas disgregadas y pensamientos desorganizados que nunca parecen cohesionarse lo suficiente como para formar un documento integrado y entendible. Lo que se recomienda es que el borrador sea redactado por un solo individuo, bien preparado en el arte de la escritura a nivel técnico y que esté familiarizado con las actividades empresariales de la organización. Si existe tal individuo, el cual puede perfectamente ser parte del comité de desarrollo, podría recibir mucha ayuda de este comité. Por ejemplo, el comité podría identificar los tópicos que necesitan atenderse, preparar un esquema de alto nivel, identificar las maneras en que la política será comunicada a los demás y proporcionar sugerencias durante la edición del documento.

A falta de cualquiera de estos dos comités, se recomiendan ciclos de revisión con los departamentos de Auditoría Interna, Recursos Humanos y Legal, ya que son importantes aliados de Seguridad Informática y serán los llamados a hacer cumplir las políticas en cuestión. Si el borrador no cuenta con la bendición de estos departamentos, es poco probable que sea tomado en serio después de su publicación. Por esta razón, es necesario reunirse con los directores de estos departamentos antes de redactar el borrador, con el fin de garantizar que todos están de acuerdo con respecto a qué debe incluir el documento de políticas. Estas reuniones se pueden llevar a cabo aun cuando haya representantes de estos departamentos en uno o en los dos comités ya mencionados.

Mientras se preparan las nuevas políticas de seguridad informática, ya debe existir un proceso adecuado de cumplimiento, o pronto ha de haber uno, porque si las políticas no pueden ser cumplidas, muy probablemente no serán eficaces. Tener políticas a cuyo cumplimiento no se puede obligar puede resultar peor que no tener ninguna, porque lo que los trabajadores pueden aprender es hipocresía y tolerancia a la conducta inadecuada. Tener políticas sin cumplimiento puede también hacer creer a la gerencia que los problemas de seguridad informática ya están atendidos o resueltos, cuando la realidad es totalmente diferente.

La gerencia a menudo cree que los trabajadores naturalmente se comportarán de manera congruente con los mejores intereses de la organización. Pero ésta es una suposición no sólo incorrecta sino peligrosa. Aunque las políticas probablemente no afecten los valores personales de los trabajadores, la gerencia las puede usar para dar a los trabajadores la oportunidad de comportarse en concordancia con los valores organizacionales. Las políticas informan a los trabajadores sobre lo que de ellos se espera, si quieren seguir allí, claro está. Suponiendo que siempre habrá distancia entre los valores personales y los organizacionales, las políticas se tomarán en serio sólo si existen mecanismos eficaces que obliguen a su cumplimiento.

Antes de la emisión de nuevas políticas, es necesario encontrar las maneras de lograr el cumplimiento a través de conversaciones con el departamento de Auditoría Interna o el de Auditoría de Tecnología Informática. Se podrían incluir herramientas como los sistemas de gestión de las licencias que vigilan el cumplimiento. También hay que considerar la dificultad y necesidad de conducir supervisiones físicas periódicas del cumplimiento. La manera y los medios para lograr esta supervisión también debe discutirse previamente. Las políticas de Recursos Humanos, tales como el proceso disciplinario y las de evaluación del desempeño del empleado, son otras que necesitan discutirse antes del desarrollo de las políticas.

Se puede apoyar el cumplimiento si existen herramientas computarizadas que ayuden al usuario. Por ejemplo, en algunas organizaciones, los servidores intranet soportan acuerdos de confidencialidad (NDC, por sus siglas en inglés) autorizados por la gerencia y disponibles para todos los empleados. Cada vez que se necesite un NDC, el usuario simplemente lo baja y lo imprime desde el servidor. La rápida disponibilidad de las herramientas ciertamente ayuda, porque los usuarios transforman las políticas de seguridad en acción.

Obligar al cumplimiento no tiene por qué ser un proceso doloroso. Considere el uso de procedimientos especiales para transmitir la idea. Por ejemplo, si alguien deja información confidencial sobre un escritorio, la información sólo puede ser devuelta si el trabajador sigue las instrucciones indicadas. La segunda vez que deje ese tipo de material por ahí, tiene que ir a buscar la información conjuntamente con su gerente. La tercera vez tiene que ir, además del gerente, con un vicepresidente. La cuarta es razón para el despido.

Las medidas para obligar al cumplimiento son a menudo más eficaces si los trabajadores están al tanto de lo que significa una violación o quebrantamiento de una

política de seguridad informática, y exactamente qué penalización esperar si los atrapan. Estas expectativas se pueden aclarar a través de programas de concientización de la seguridad, como parte integral de las mismas políticas. Dichos programas podrían, por ejemplo, decir claramente que la información es propiedad de la Empresa X, y que no debe ser copiada, modificada, borrada o utilizada para cualquier otro fin sin la autorización de la gerencia.

No se debe intentar modificar o influenciar de manera positiva la conducta de los trabajadores. La intención no es “atrappar” a la gente y aplicar el peor castigo a los “criminales”. Aunque debe usarse el castigo, la intención de los mecanismos de cumplimiento no es la de generar grandes cantidades de no cumplidores. Si mucha gente no cumple, eso quiere decir que las políticas están fallando. En estos casos, hay que comunicar mejor la intención de las políticas o modificarlas para adaptarlas mejor a las circunstancias y a la cultura organizacional.

Cumplimiento Automatizado de Políticas Mediante Servidores de Políticas

En muchas organizaciones, la complejidad de los sistemas informáticos está sobrepasando la capacidad del personal para manejarlos. Para enfrentar esta situación, se están creando nuevas herramientas de sistemas expertos. Por ejemplo, ahora algunos cortafuegos incluyen un sistema experto que le dirá al técnico instalador si la configuración adoptada originó una vulnerabilidad en el sistema. Para manejar esta mayor complejidad, las organizaciones necesitarán sistemas de gestión centralizados que jueguen un papel más importante en la seguridad. Por ejemplo, los sistemas de administración de redes de algunas organizaciones actúan como conducto para transmitir la detección de un intruso al operador de guardia.

Un nuevo e interesante desarrollo en este sentido es el llamado servidor supervisor de políticas. Los servidores de políticas toman las políticas de la organización y las codifican en lenguaje especial de máquina que puede ser luego accedido por distintos sistemas operativos, paquetes de control de acceso y otros sistemas de administración de redes. Ejemplos de estas políticas o reglas incluyen el mínimo de caracteres de las contraseñas, la máxima cantidad de intentos de iniciar una sesión, y si los anexos de los correos deben pasar por los cortafuegos. Es decir, el servidor de políticas funcionará como un diccionario de datos, porque se le pedirá que proporcione las instrucciones definitivas desde un punto centralizado. En un futuro cercano, suites de productos de un solo proveedor, o la

combinación de varios proveedores, comenzarán a realizar las tareas racionalizadoras y centralizadoras de un servidor de políticas.

Para prepararse para los acontecimientos venideros, se debe considerar cómo las políticas desarrolladas hoy serán colocadas en los modelos de computadores del mañana. Se debe intentar ser lo más lógico y directo posible, porque no sólo ayudará a los lectores a entender cómo comportarse en lo relativo a la seguridad informática, sino también ayudará a los programadores del

mañana en la creación de reglas que se puedan hacer cumplir a través del computador. También se debe intentar lograr la mayor coordinación de las políticas de seguridad informática entre las distintas organizaciones, las diferentes redes, los complejos sistemas y las cambiantes plataformas. Esto también reducirá la complejidad y permitirá a las organizaciones adoptar más fácilmente las nuevas herramientas de cumplimiento de las políticas.

Cronograma para el Desarrollo de las Políticas

Antes de embarcarse en el proyecto de redactar y obtener la autorización gerencial para las políticas de seguridad informática, es recomendable clarificar quién es el responsable de emitir y hacer cumplir las políticas. Solamente puede iniciarse la tarea cuando existe una clara asignación de responsabilidad de cumplimiento de las políticas de seguridad informática. Muchas veces esto significa la necesidad de preparar y aprobar un enunciado de la misión por parte del grupo centralizado de seguridad informática antes de llevar a cabo el esfuerzo de redacción de las políticas. Si la responsabilidad no ha sido asignada, entonces considérelo el primer paso. Si este importante paso es ignorado, prepárese a recibir una andanada de politiquería interna que muy probablemente retrasará significativamente cualquier progreso en la redacción de las políticas.

Otro prerrequisito necesario para redactar exitosamente las políticas de seguridad informática consiste en la perspectiva de la gerencia. Solamente cuando la gerencia note que la información en sí misma se ha convertido en factor crítico de producción es que la seguridad informática será reconocida como un asunto digno de su atención. Esta perspectiva también se conoce por varias frases, incluyendo "gestión de los recursos informáticos" y "reconocimiento de la información como activo". La gerencia debe reconocer que es responsable del manejo de la información misma. Históricamente, la gerencia ha creído que la información sirve para manejar otros recursos, tales como las personas. La gerencia tiene que apreciar la necesidad de nuevas herramientas y técnicas en el manejo de la información misma. En medio de este intercambio, es apropiado mencionar la contribución significativa que pueden aportar las políticas en este sentido. Si la gerencia no entiende cuán importante es la información para su organización, es poco probable obtener su apoyo para los esfuerzos de redacción de políticas de seguridad

informática. Para mayor información sobre este tópico, ver "[Objetivos y Alcance de las Políticas](#)" en la página 31.

La gerencia debería reconocer la existencia de problemas de seguridad informática, y que necesita de políticas para atenderlos, pero esto tiene que ocurrir antes de iniciar un esfuerzo serio de redacción de políticas. Aunque pueda parecer obvio, muchos esfuerzos bien intencionados de redacción han fracasado por no haber establecido el piso fundamental. Este piso fundamental muchas veces incluye una breve presentación de concientización. Los tópicos de dicha presentación pueden incluir los riesgos que la organización enfrenta, el historial de pérdidas, los incidentes sufridos por otras organizaciones del mismo ramo y los enfoques aceptados para enfrentar estos riesgos e incidentes en seguridad informática.

Lo ideal sería que el esfuerzo de desarrollo de las políticas se iniciara después de la presentación de una evaluación de gran alcance de los riesgos presentes en seguridad informática. La evaluación de riesgo debe indicar, tal vez sólo en términos de alto nivel, el valor de la información, los riesgos a los cuales la información está supeditada y las vulnerabilidades asociadas con la forma actual de manejar la información. Una evaluación de riesgo aportará información útil de antecedentes, lo cual podrá ser usado al momento de seleccionar las políticas de este manual. Pueden incluirse en la introducción o prefacio del documento de políticas de seguridad informática, los tipos generales de amenazas que enfrenta la organización y demás antecedentes provenientes de las evaluaciones de riesgo.

Uno de los mejores momentos para desarrollar una política de seguridad informática es cuando se está preparando un manual de seguridad informática, ya que al ser distribuido en toda la organización es el mejor sitio para colocar las políticas de seguridad informática.

Se pueden preparar políticas específicas escritas también justo antes de recopilar el material necesario para el adiestramiento y concientización de los usuarios. Estas actividades pueden incluir cintas de video, charlas, afiches o artículos periodísticos de la compañía. Para mayor información sobre el desarrollo de políticas de seguridad, ver Apéndice D, “[Lista de Métodos Sugeridos para Aumentar Nivel de Conciencia](#).”

Otro buen momento para preparar las políticas es justo después de una violación importante de la seguridad informática, después de un informe desfavorable de auditoría relacionado con los computadores, de una demanda judicial relacionada con la seguridad o después de cualquier otro tipo de pérdida que reciba mucha atención de la alta gerencia. Este es un buen momento para adelantar el desarrollo de las políticas ya que la gerencia estará especialmente receptiva y preocupada por apoyar la seguridad informática. En estos momentos es importante obrar rápidamente, ya que el nivel de preocupación declina exponencialmente.

Con el fin de proporcionar dirección a la preparación de los lineamientos del desarrollo de sistemas, los memorandos de implementación de paquetes de control de acceso, las normas técnicas de computación, las descripciones procedimentales de control interno y otros documentos más específicos de seguridad informática, las políticas deben prepararse al inicio del ciclo de vida del esfuerzo de redacción. Un conjunto inicial de políticas es usualmente breve, seguido de enunciados

más detallados dirigidos a áreas específicas de preocupación. Ejemplos son las políticas de teletrabajo, las políticas de Internet y las políticas para el desarrollo de aplicaciones por usuarios.

Un buen objetivo a recordar cuando se redactan las políticas es evitar modificarlas durante tres años. Esto se debe a los rápidos cambios en el área de sistemas informáticos, donde las políticas son modificadas a sólo un año o dos de ser emitidas. Para evitar su rápida obsolescencia, las políticas deben redactarse independientemente de los productos comerciales específicos, de los proveedores y de las estructuras organizacionales. Independizarse de estas áreas no excluye la inserción de enunciados generales referidos a las mismas áreas en el documento. Por ejemplo, la necesidad de contraseñas dinámicas se menciona frecuentemente en los documentos de políticas, pero no los proveedores ni los productos mismos.

Dada la rapidez de cambio en este campo, es recomendable tratar de lograr que la gerencia asigne tiempo para hacer las modificaciones correspondientes a las políticas de seguridad informática en uno o dos años. También dado que es necesario actualizar las políticas de seguridad informática, este manual se actualiza cada cierto tiempo. Si usted se encuentra utilizando una versión no actualizada, le recomendamos visitar la casa editora para obtener información sobre la disponibilidad de la última versión.

Longitud del Documento de Políticas

Determinación de la Cantidad Adecuada de Políticas

Para ser eficaces, las políticas de seguridad informática deben ser elaboradas a la medida de las necesidades peculiares de la organización. Algunas organizaciones tienen muchas políticas, mientras otras tienen sólo unas pocas. Por ejemplo, el manual de política de seguridad informática de una importante compañía telefónica tiene más de 150 páginas, el de una gran compañía aeroespacial tiene 75 páginas, y el de una muy conocida compañía ferroviaria tiene 25 páginas. Si bien la cantidad de páginas de las distintas organizaciones varía, la tendencia clara es hacia documentos más detallados y, por consiguiente, más extensos.

La categoría de la industria es un determinante crítico de la cantidad de páginas de un documento de políticas, así como también lo es el punto de vista gerencial sobre la centralización de la función de seguridad informática. Si

se valora y estimula la discreción de la gerencia local, el documento generalmente será menos detallado y por lo tanto más corto. Si por el contrario, es el control centralizado el que se valora y estimula, entonces un documento de políticas generalmente será más detallado y por lo tanto más extenso. La mayoría de las organizaciones tienen una combinación de estas dos, donde ciertas actividades de seguridad son manejadas de manera descentralizada, y otras de manera centralizada. Por ejemplo, los coordinadores de seguridad informática local pueden manejar la emisión de identificadores de usuario y reinicializaciones de contraseñas a nivel departamental, pero el personal centralizado puede usarse en asuntos de la seguridad de la red, tales como el mantenimiento de cortafuegos.

Algunos equipos gerenciales piensan que es apropiado estar claro sobre estos asuntos. En esos casos, puede haber necesidad de muchas políticas. Algunos gerentes

son renuentes a tener muchas políticas, prefiriendo depender del criterio profesional de los trabajadores. Otros gerentes querrán mantener el documento breve porque temen que los trabajadores piensen que no se les tiene confianza. Pero no se preocupe demasiado en minimizar el impacto del documento sobre la cultura corporativa. Algunos requisitos básicos de seguridad informática deben ser comunicados a través de una política, aunque provoquen preguntas difíciles.

Las audiencias a atender pueden tener un alto nivel de instrucción, tales como las de un instituto de investigación, en cuyo caso podría ser necesario más material escrito. Las audiencias pueden poseer un nivel marginal de instrucción, como la de una organización manufacturera que emplea inmigrantes de varios otros países, y menos material escrito. Una organización puede estar habituada a documentar los procesos internos de negocios, en cuyo caso generalmente será apropiado tener más políticas. Por otro lado, una organización podrá optar por mantener deliberadamente la documentación a un mínimo, lo cual generalmente significa menos políticas.

Aunque es más probable que la gente lea completamente un conjunto conciso de políticas, hay mucho que decir a favor de un conjunto completo de políticas de seguridad informática. Por ejemplo, para un patrono sería más fácil defenderse en un tribunal de las acusaciones de invasión a la privacidad hechas por sus empleados si sus políticas fueran explícitas. Por otro lado, y de mayor importancia aún, un conjunto completo de políticas aporta la orientación definitiva que requieren los trabajadores. La orientación definitiva en un extenso enunciado de política puede ser de bastante utilidad en un tribunal cuando haya la necesidad de evidenciar que la gerencia ha sido diligente en su atención a la seguridad informática. Los enunciados más extensos son también de ayuda en las acciones disciplinarias porque definen explícitamente los patrones de conducta esperados.

Otro factor que afecta la longitud del documento de políticas proviene de las expectativas de la gerencia hacia un documento de alto nivel o de bajo nivel. Un documento de alto nivel típicamente definiría las responsabilidades de los trabajadores y unas cuantas medidas importantes como las tarjetas de contraseñas dinámicas. Un documento de bajo nivel típicamente entraría en más detalle y haría referencia tanto a tareas como a procedimientos. Si no existe orientación de la gerencia sobre este punto, asegúrese de clarificar este detalle antes de preparar el bosquejo del documento de políticas.

La tecnología internet e intranet también modifica el tamaño de los documentos de políticas. En el pasado, los documentos eran enviados a los trabajadores en papel solamente, pero ahora pueden residir en el servidor de intranet y el trabajador puede tener acceso a ellos cuando lo necesite. Esto significa que los documentos pueden ser más detallados de lo que eran antes sin imponer una carga adicional sobre los trabajadores. Igualmente, los enlaces instantáneos que aporta esta tecnología facilitan el establecimiento de interconexiones entre documentos, permitiendo a los usuarios ubicar con más rapidez el material que les interesa.

Una estrategia general para minimizar el tamaño del documento consiste en mencionar las prohibiciones solamente. Con esta estrategia, los lectores del documento de políticas oirán primordialmente lo que no deben hacer y no tanto lo que sí deben hacer; aunque esta regla tiene sus excepciones. Por ejemplo, los trabajadores deben informar los incidentes de seguridad a alguien que pueda aplicar el correctivo apropiado. Esto es algo que los trabajadores deben hacer, y no algo que no deben hacer. Pero en general esta estrategia tiene su mérito. Con esta estrategia se minimiza el tamaño del documento, porque el conjunto de prohibiciones es considerablemente inferior al conjunto de acciones que supuestamente sí deben realizar los trabajadores. Por consistir en instrucciones mínimas, esta estrategia permite más flexibilidad a medida que cambian las actividades empresariales. Siempre que los sistemas no cambien significativamente, tales instrucciones pueden ser relevantes.

Como principio de redacción de políticas, es conveniente emitir sólo aquellas políticas absolutamente necesarias, porque las personas son inherentemente diferentes, así como lo son los grupos formados por ellas. Tener sólo aquellas políticas absolutamente necesarias permite la iniciativa personal, la creatividad y la manifestación de la expresión. Aunque es cierto que los seres humanos tienen la tendencia de generalizar y de normalizar, frecuentemente este concepto se lleva a extremos. Un ejemplo sería una organización que tiene tantas políticas de seguridad y tantos procedimientos que no se puede hacer el trabajo. Entonces, considere seleccionar un conjunto mínimo de políticas para toda la organización, y luego deje el resto a la discreción de la gerencia departamental, divisional o de las otras gerencias locales.

En vez de comenzar globalmente, es mejor concentrarse sólo en lo esencial, produciendo así instrucciones concisas. Luego, a medida de las circunstancias, se van agregando políticas adicionales. Este enfoque a menudo significa la emisión de enunciados separados dirigidos a

áreas problemáticas, tales como Internet y el teletrabajo. Porque solicita menos concesiones en un momento dado, este enfoque 'por fases' tiene mayor probabilidad de ser aprobado por la gerencia y de ser cumplido por los usuarios. Tanto la visibilidad como la buena reputación de un esfuerzo de seguridad informática tienen mayor probabilidad de mantenerse en altos niveles con este enfoque por fases, ya que obligan a obtener aprobación frecuente y retroalimentación.

La mejor manera de proteger la información y los sistemas informáticos siempre dependerá de las circunstancias. Factores como el tipo de usuario, la configuración del equipo de computación, y cuán confidencial es la información, dictarán lo que debe hacerse en materia de seguridad informática. Aunque algunas personas quisieran lo contrario, las políticas nunca podrán definir el camino verdadero y óptimo para resolver todas las situaciones, todo el tiempo. Una mente abierta y la disposición de manejar las circunstancias facilitan la búsqueda de soluciones aceptables en seguridad informática. Un conjunto global de políticas que niegue la responsabilidad personal está destinado a inhibir la seguridad informática, cuando no a generar rebeldía y desdén. Trate de redactar una política que brinde un mínimo de orientaciones, pero que a la vez permita respuestas específicas para la situación que se presente.

Otra manera de determinar la cantidad adecuada de políticas tiene que ver con la intención de hacer la seguridad informática tan transparente al usuario como sea posible. Mientras más transparente es la política, más rápido se acepta. Mientras más transparente, menos necesidad hay de tener políticas escritas. Las políticas, en la mayoría de los casos, atienden áreas para las cuales los proveedores no ofrecen soluciones automatizadas transparentes para el usuario; es decir, donde debemos depender de los usuarios y de otros trabajadores. Cuando los proveedores proporcionen soluciones de seguridad informática transparentes multiplataforma y suficientemente confiables, habrá una reducción significativa de la necesidad de tener políticas escritas. Ese mundo ideal parece estar a muchos años de distancia todavía; así que, mientras tanto, seguirán haciendo falta unas cuantas políticas.

La cantidad de políticas a producir también es función de las audiencias involucradas. Muchas organizaciones preparan varios documentos; uno para los usuarios, otro para la gerencia y otro para el personal técnico. Muchas de las políticas de cada documento serán iguales, aunque el grado de detalle, las palabras técnicas utilizadas y la cantidad de ejemplos varíen. Si la audiencia está conformada por usuarios finales, la

cantidad de políticas debería estar limitada a unas cuantas páginas. Para la gerencia, hay consideraciones adicionales, tales como los asuntos legales, lo cual debería extender el tamaño del documento. Para el personal técnico, el documento será probablemente mucho más largo, detallado y técnico. **En este manual se han segmentado los públicos después de los comentarios sobre las políticas con el fin de prestar más ayuda al respecto.**

Otro factor que afecta la cantidad de políticas necesarias es el grado de seguridad que requiere la organización. Como indicador general, mientras más intensas en términos de información sean las actividades de una organización, mayor será la necesidad de seguridad. Por ejemplo, un banco tendrá muchas políticas, mientras que una cadena de tiendas de café tendrá pocas. Las actividades delicadas, tales como las de sostenimiento de la vida o las de defensa nacional, también aumentan la necesidad de seguridad. Una organización con poca necesidad de seguridad, como una empresa de lavado de automóviles, generalmente tendrá pocas políticas, y habrá implementado pocas medidas de seguridad. Por otro lado, una organización con significativas necesidades de seguridad, como una empresa de seguros, tendrá más políticas, y habrá implantado muchas medidas de seguridad informática.

La mayoría de las políticas aquí discutidas, aunque orientadas primordialmente a comercios y empresas, son aplicables a cualquier organización. Algunas son relevantes sólo para las organizaciones con ciertos niveles de seguridad. En este manual, al final del comentario de cada política se indica el tipo de ambiente donde mejor se puede utilizar la política.

Determinación de la Longitud de Cada Política

Más allá de la cantidad de políticas, se debe considerar la longitud de cada política. Las políticas incluidas en este documento están deliberadamente redactadas en una sola oración. Esta declaración concisa de políticas promueve la aceptación por parte de los trabajadores, porque es una sola instrucción fácil de leer y de entender. Mantener los enunciados concisos también enfatiza que las políticas proporcionan una orientación general, no los detalles de cómo manejar cada circunstancia previsible. Los detalles usualmente aparecen en los documentos de normas o en los manuales de procedimientos operativos.

Otra consideración con respecto a la longitud de las políticas es que necesitan ser lo suficientemente específicas como para ser comprendidas e interpretadas de manera uniforme. Al mismo tiempo, las políticas no

deberían ser tan específicas como para negar a la gerencia local la oportunidad de adaptarlas a sus condiciones. Por ejemplo, la gerencia puede emitir una política que especifique que todos los usuarios deben poseer contraseñas difíciles de adivinar por terceros no autorizados. Esta política le da espacio a la gerencia local para determinar si quiere usar contraseñas generadas por el sistema, o si quiere que los propios usuarios seleccionen sus contraseñas, acompañadas quizás por un mecanismo que garantice que los usuarios están haciendo un buen trabajo.

La longitud de cada política es el reflejo de cuántas opciones quiere especificar la gerencia. Por ejemplo, la gerencia puede especificar que es suficiente que todas las conexiones a la red interna tengan un cortafuego o cualquier otro sistema autorizado de control de acceso, o puede incluir el tipo de cortafuego a utilizar, como uno de filtrado de empaques o uno de filtrado de aplicaciones. La gerencia también puede incluir qué tipo de servicios se pueden transmitir a través del cortafuego. Generalmente, se recomienda mantener los enunciados o instrucciones de las políticas a niveles relativamente altos, y dejar los detalles, tales como los descritos en las dos últimas preguntas, para los documentos suplementarios o de normas. Esto significa no solamente que la política será aprobada con mayor rapidez, sino que la política no necesitará modificarse una y otra vez a medida que cambien las circunstancias.

Para aquellos con necesidad de producir documentos de políticas de muchas especificaciones, las posibles opciones deben identificarse y evaluarse antes de redactar la política. Revisar todas las opciones de cada política con la gerencia generalmente deviene en la prolongación del proyecto. En lugar de ello, una forma fácil de proceder sería tomar decisiones técnicas con un pequeño grupo de empleados, tal vez en un Comité de Gestión de Sistemas Informáticos. Por cada política controversial, el pequeño grupo puede preparar una lista de opciones, indicando los pros y los contras. Esta lista se mostraría a la gerencia para lograr la pre-aprobación. Este enfoque aumentaría significativamente la probabilidad de aprobación de la política final, dado que los puntos controversiales ya han sido pre-vendidos con la entrega previa de listas suplementarias y discusiones realizadas.

Algunas organizaciones podrían decidir incluir ejemplos específicos para aclarar la política, aunque hacerlo alargará la extensión de cada enunciado. Como ilustración de este enfoque, una política que prohíba el uso personal del sistema de información de la Empresa X podría estar acompañada de ejemplos como jugar en

Internet o el uso de los teléfonos de la organización para socializar. Aunque los ejemplos convierten a la política en algo real y tangible, también reducen significativamente los errores en la interpretación y en la aplicación de una política. Pero, a la vez, los ejemplos podrían parecer degradantes, redundantes e innecesarios a algunos lectores. En la mayoría de los casos, no se suministran ejemplos con las políticas, excepto en aquellas circunstancias donde se supone habrá confusión o disputa.

Otro aspecto importante que puede afectar la longitud del documento son las explicaciones de las intenciones de las políticas. Si van a apoyar las políticas de seguridad informática, los trabajadores necesitan saber por qué son importantes. La cantidad de material necesario para transmitir la intención de las políticas puede variar considerablemente, dependiendo de la audiencia a la cual se dirijan. A medida que se discuta cada vez más la seguridad informática en los medios noticiosos, la audiencia en general comenzará a apreciar los riesgos. Esto significa que la cantidad de palabras necesarias para explicar las intenciones de un documento de política decrecerá significativamente. En caso de necesitarse, la intención completa de cada política puede encontrarse en la sección de comentarios de cada política en este manual. En la mayoría de las organizaciones, las intenciones son comunicadas en las sesiones de adiestramiento, en el software de capacitación asistida por computadores, u otros medios diferentes a la política escrita.

Otras partes del documento de seguridad informática no mencionados anteriormente, pero que podrían contribuir significativamente al tamaño del documento, incluyen el marco teórico, la tabla de contenido, el índice, el glosario, un organigrama relacionado con la seguridad informática, una declaración de las responsabilidades de seguridad informática, una lista de documentos internos relevantes, una descripción de la metodología de la evaluación de riesgo, un conjunto de normas de seguridad de sistemas informáticos, un conjunto de procedimientos de seguridad informática, un resumen de las modificaciones de los documentos y el estudio de un caso indicando cómo debe aplicarse el material. Los materiales específicos a incluir en el documento de políticas tienen que determinarse a través de las necesidades de la organización, la sofisticación en el área de seguridad informática, los documentos ya divulgados y las responsabilidades del grupo que prepara las políticas. Un documento de políticas de seguridad informática que incluya todos los materiales mencionados puede extenderse hasta 100 páginas o más.

Proceso Iterativo de Desarrollo

Si se requiere un conjunto de políticas de mayor alcance, se recomienda un proceso de dos etapas. La primera etapa consiste en obtener la aprobación gerencial para un conjunto generalizado de políticas, y la segunda etapa consiste en la aprobación de un conjunto más específico de políticas. El conjunto generalizado incluiría sólo unas 30-50 políticas, mientras que el conjunto específico incluiría unas 50-100 políticas adicionales. Un ejemplo de la política generalizada sería la necesidad de identificar positivamente a todos los usuarios antes de darles acceso a los sistemas internos. Un ejemplo de una política específica sería la necesidad de utilizar tarjetas de identidad que generen contraseñas dinámicas cada vez que el usuario se conecte a la red interna desde una ubicación externa. De manera de poder cubrir ambas situaciones, este manual contiene tanto políticas generales como específicas.

Un proceso de dos etapas también es aconsejable debido a que permite al grupo de seguridad informática concentrar su atención inicial en modelos conceptuales fundamentales, tales como la propiedad de la información y la clasificación de la sensibilidad de los datos. Después de que estos modelos conceptuales han sido enfatizados a través de un documento inicial de políticas y después de haber sido comunicados por medio de un programa básico de concientización de la seguridad informática, los requisitos más detallados pueden expresarse en un documento de políticas más amplio. Se emplee o no este enfoque de dos etapas, deben identificarse los modelos conceptuales fundamentales en que se basan las políticas. Estos modelos conceptuales también deben ser incluidos en el documento de políticas o en cualquier otro material previamente comunicado a las audiencias respectivas.

Se recomienda tomar en cuenta a la audiencia correspondiente al momento de desarrollar las políticas. Las políticas generalmente se pueden dividir en dos: las dirigidas a los usuarios finales y la gerencia, y las dirigidas a los programadores, diseñadores de sistemas y otros técnicos. La primera audiencia debería incluirse en el primer intento de desarrollo de políticas, mientras que los esfuerzos siguientes atenderían a la segunda audiencia.

Si el conjunto inicial de políticas enviado a la gerencia es demasiado largo o severo, la gerencia puede rechazarlo. Como resultado, la ventana para obtener políticas puede cerrarse por cierto período. Por ello, el primer conjunto de políticas debe ser breve y relativamente fácil de cumplir. Luego, cuando el primer conjunto ha sido

apoyado e implantado en toda la organización, se puede preparar una lista más completa y más estricta. Es mucho mejor proceder lentamente con una serie de esfuerzos de desarrollo, de manera de obtener credibilidad y frecuente comunicación con la gerencia, que preparar un gigantesco documento de políticas que luego sea rechazado por tener demasiadas palabras, demasiado rápido y demasiado pronto.

Se sugiere que las políticas se redacten utilizando la clásica estrategia de ensayo y error para el manejo de problemas complejos. Después de emitir una política breve, deben observarse los efectos de la misma, incluyendo las reacciones de los usuarios y los problemas en el cumplimiento. Los efectos no deseados deben corregirse emitiendo políticas nuevas o modificadas. Deben notarse entonces los efectos de dichas correcciones y nuevamente corregirse para eliminar cualquier efecto colateral no deseado.

Las políticas deben revisarse periódicamente, por lo menos una vez al año, para garantizar que siguen siendo relevantes y eficaces. Es importante eliminar la políticas que ya no sean aplicables. Tanto la gerencia como los usuarios estarán agradecidos de los esfuerzos que se hagan para simplificar las políticas, porque estos esfuerzos también mejoran la credibilidad de la función de la seguridad informática dentro de la organización. Los trabajadores apreciarán que el personal de seguridad no esté buscando establecer una burocracia, sino fijar los controles mínimos necesarios para proteger los activos informáticos de la organización.

Los retrasos asociados con el proceso de aprobación de las políticas de seguridad informática pueden generar niveles entendibles de frustración. Porque, aun cuando se haya hecho un trabajo respetable en el desarrollo de las políticas, la gerencia a menudo toma un largo tiempo para revisarlas y aprobarlas. A pesar de que la seguridad informática se discute con frecuencia en la prensa y TV, la plena mayor de muchas organizaciones simplemente no la entiende. Partes de algunas de estas publicaciones sobre la necesidad de tener políticas pueden mostrarse a la gerencia mientras se hace la larga espera por la aprobación. Esto mantendrá el tópico en el tapete, y reforzará la presión sobre la gerencia para que preste atención a los asuntos de seguridad informática.

Tabla de Contenido de un Típico Documento de Políticas

Las secciones reales de un documento de políticas variarán considerablemente de organización a organización. Esto debe ser un reflejo de los factores específicos de cada organización, tales como la sensibilidad, el

valor y cuán crítica es la información a proteger. También deben considerarse la naturaleza de los sistemas, las actividades empresariales, las leyes y costumbres locales, y varios otros factores. En muchas organizaciones habrá varios documentos, cada uno para un público diferente. Para mayor información acerca de la creación de un documento de políticas, ver “[Preparación de una Matriz de Cobertura](#)” en la página 15.

Si bien debería evitarse la duplicación, siempre habrá algo de redundancia en el documento de políticas, sin importar qué tipo de modelo se seleccione.

Las secciones típicas de un documento de políticas son: la definición de seguridad informática, la declaración de la intención de la gerencia de apoyar los esfuerzos de seguridad informática, y la definición de las responsabilidades gerenciales generales y los deberes organizacionales específicos con respecto a la seguridad informática. También deben incluirse las políticas propiamente dichas, con o sin ejemplos y explicaciones. Algunos documentos de políticas pueden incluir una discusión sobre los procesos de supervisión del

cumplimiento y medidas disciplinarias. También puede haber mención de las maneras de informar o manejar las situaciones de incumplimiento. Una lista de los documentos propios relacionados con este tópico puede ayudar a los que deseen mayor información.

Aunque no es muy común, se puede incluir una tabla que muestre las circunstancias cuando se pueden aplicar ciertas políticas, como ayuda adicional para los lectores del documento. Por ejemplo, cuando se envía por correo un documento que contiene información confidencial, se aplica la política A; pero cuando se envía por courier, se aplica la política B. Para mayor información acerca de este tipo de tabla, ver Capítulo 17, “[Modelo de Tabla de Referencia Rápida de Clasificación de Datos](#). ” Estas tablas pueden recibir el formato de las tablas de decisión. En lugar de referenciar las políticas específicas, la tabla de decisión podría contener números que hacen referencia a las secciones del documento de políticas. Existen muchos modelos que puede utilizarse para crear la base de los documentos de políticas de seguridad informática. La lista correspondiente se ubica en la [Tabla 2-3](#).

Tabla 2-3: Modelos de Documentos de Políticas

Modelo de Documento de Políticas	Enfoque del Documento
Enfoque sobre los atributos de la información	Confidencialidad, integridad y disponibilidad
Propiedad y custodia de la información	Roles y responsabilidades
Condición laboral del lector	Empleado, contratista, consultor, temporal, socio, cliente
Cargo	Administrador de sistemas, desarrollador de sistemas, usuario, gerente
Clasificación de los datos	Sensibilidad de la información
Tiempo requerido para restablecer esquema	Criticidad de los datos
Valoración de la información	Valor del recurso
Tipos de amenazas	Orientación legal o empresarial
Tipos de equipos de computación	Mainframes y computadores personales
Ubicación geográfica	En la oficina o en la vía
Dominios en redes	Diferentes controles en distintos dominios
Decisiones que la gente enfrenta	Cuán a menudo respaldar y cómo evitar problemas con virus

Cuáles Temas Atender Primero

La complejidad del mundo de la seguridad informática puede ser abrumadora para una organización que apenas esté empezando a tomarla en cuenta. Para hacerlo más fácil a los usuarios, gerentes y otros grupos quienes no están familiarizados con la seguridad informática, sólo se deben emitir unas cuantas políticas esenciales al principio. Luego, a medida que aumenten el entendimiento y el apoyo, se pueden emitir políticas adicionales. Un ejemplo de este tipo inicial de política de seguridad informática se encuentra en el Capítulo 4, “[Modelo de Política de Seguridad Informática de Alto Nivel](#).”

Recomendamos, sin embargo, que en lugar de copiar la política que aparece en el Capítulo 4, “[Modelo de Política de Seguridad Informática de Alto Nivel](#),” se brinde consideración a los tópicos o temas con mayor necesidad de ser atendidos. Como son distintos en cada

organización, éstos son los temas que deberían incluirse en el enunciado inicial de política. Típicamente, dichos temas incluyen, como mínimo, la responsabilidad de Seguridad Informática, los virus computacionales, el respaldo de la información, la planificación de contingencias, la interconexión de los sistemas, la identificación de los usuarios y los privilegios de control del acceso a los sistemas.

Otra forma de ver un enunciado inicial de política es que debe establecer la base de un esfuerzo exitoso para implantar la seguridad informática en la organización. Esta base o infraestructura organizacional incluye políticas, normas y responsabilidades, ya cubiertos en “[Garantía de Implantación de los Controles](#)” en la página 7. Se puede utilizar un conjunto inicial de políticas para establecer o aclarar partes faltantes de la infraestructura organizacional. Por ejemplo, si no existen mecanismos para obligar al cumplimiento de las

políticas, el conjunto inicial de políticas puede discutir la responsabilidad de la supervisión del cumplimiento, así como la penalización por incumplimiento.

Si ya existe un documento de políticas de seguridad informática, el reto entonces será determinar cuáles ideas novedosas o modificadas necesitan atenderse en un nuevo documento. Una de las maneras más rápidas de llegar a una decisión al respecto, es a través de una matriz de cobertura, tal como se describe en

[“Preparación de una Matriz de Cobertura”](#) en la página 15. En este caso, el documento de políticas existente puede ser diagramado como matriz de cobertura, y los números de referencia de las ideas que necesitan cambiarse pueden subrayarse o ponerse dentro de un círculo. Luego, la matriz puede completarse con las políticas que se puedan tomar de este manual, preparándose así un esquema para el nuevo documento.

Utilización de las Políticas

Audiencia Definida Como Objetivo

Las políticas de este manual están dirigidas a aquella persona con suficiente conocimiento de computación como para desempeñarse en un ambiente relacionado con la seguridad informática. Estas suposiciones permitieron la supresión de muchas palabras comunes en sistemas de computación y comunicación, tales como “Proveedor de Servicios de Internet”. Hasta donde se pudo, tanto los acrónimos como los términos técnicos utilizados en sistemas de computación y comunicación se han omitido deliberadamente, porque estas políticas deben ser aprobadas por la gerencia, donde puede haber extensa falta de conocimiento al respecto. Por otro lado, a los usuarios poco interesan los términos técnicos.

Adaptación de las Políticas

Las políticas de este manual deben ser revisadas y comparadas con las de la organización. Mediante el uso de un procesador de palabras cualquiera, las políticas que parezcan calzar dentro de la organización pueden ser extraídas con comandos recortar y pegar, y colocadas en un archivo separado. Este nuevo archivo puede entonces modificarse para reflejar las características particulares de la organización.

A lo largo de este manual se utiliza la “Empresa X”, una organización genérica que es fácilmente sustituible por el nombre de la organización que va a utilizar las políticas. A pesar de la aparente parcialización hacia la industria privada, estas políticas han sido utilizadas exitosamente por todo tipo de organizaciones, incluyendo gobiernos civiles, militares y entidades sin fines de lucro. El uso de la palabra organización no quiere decir que las políticas tienen que usarse en toda la organización, sino que pueden aplicarse en filiales, divisiones o departamentos. Sin embargo, para mantener costos bajos y continuidad administrativa debe intentarse la aplicación más amplia posible de las políticas.

Las políticas de este manual están redactadas de manera deliberada en términos generalizados. Por ejemplo, muchas políticas son igualmente aplicables a estaciones de trabajo sin discos, computadores personales, super-servidores, minicomputadores y mainframes. En lugar de restringir la política a sólo un tipo de computador, es preferible una política generalizada porque fomenta la protección uniforme de la información, sin importar dónde resida, el tipo de tecnología ni la forma de la información. Los términos de búsqueda son generales, tales como “red” en lugar de estrechos, tales como “red de área local”. El esfuerzo detrás de la política debe simplificarse tomando una perspectiva independiente de la plataforma y creando un conjunto de políticas que se pueda aplicar a todos los ambientes. Tomar una perspectiva independiente del hardware y del software también evitará la necesidad de actualizar el documento si cambia el ambiente informático.

Las políticas de este manual generalmente toman una posición muy estricta con respecto a la seguridad informática, y pueden ser muy severas para la mayoría de los ambientes. Las políticas deben ser eliminadas, modificadas o diluidas para satisfacer las necesidades de la organización. En todo este material se usó la forma más fuerte, porque es más sencillo suavizar una política estricta que fortalecer una débil.

Uso de la Búsqueda Mediante Palabras Clave

Una de las características más útiles de este manual y su CD-ROM anexo es la capacidad de proporcionar búsquedas por palabras clave para ubicar las políticas de interés. Si la organización quiere atacar un área específica, digamos que por casualidad son los virus, puede identificar todas las partes donde se menciona este tema, utilizando la opción de búsqueda del CD-ROM. El CD-ROM contiene toda la información del manual.

Al realizar las búsquedas, asegúrese de utilizar sólo los caracteres principales. Por ejemplo, si estamos interesados en redes, utilizamos la versión singular, red, en lugar de la plural, redes. Esta acción ubicará tanto los singulares como los plurales y los términos relacionados, tales como “en red”. Se recomienda hacer intentos de búsqueda con los singulares más significativos de la frase en vez de todas las palabras. Por ejemplo, la palabra clave es “diligencia” para buscar “diligencia debida.”

También se recomienda el uso de sinónimos en las búsquedas. Por ejemplo, si la búsqueda tiene que ver con asuntos de la confidencialidad de la información, use “confidencialidad”, “secreto”, “restringido” y otros términos relacionados. Para que sea más probable encontrar lo que se busca, los términos utilizados en este manual son generalmente aceptados y poco técnicos.

Otro consejo para la búsqueda en el CD-ROM la constituye el uso de palabras truncadas en lugar de palabras completas. Si la búsqueda incluye verbos o sustantivos con formas irregulares se recomiendan iniciar varias búsquedas, cada una con una forma diferente de la palabra.

Con el fin de cubrir tanto terreno como se pueda, lograr enfoques consistentes a la seguridad informática y simplificar la ya complicada vida de la gente que trabaja en este campo, las políticas de este manual se han redactado con terminología general y no con terminología específica. Por ejemplo, en lugar de utilizar términos parecidos a “Red de Área Local”, “Puertas de Enlaces” o “Router”, se han empleado términos más generales como “Red”.

Objetivos y Alcance de las Políticas

Objetivos Motivacionales

En la mayoría de las organizaciones, la información representa uno de los activos primarios en riesgo. Estudios recientes muestran que, en las economías industrializadas, del 10% al 95% de los activos de una organización cualquiera están relacionados con el manejo de la información. Los riesgos a las personas, a los equipos, a los edificios, a la tierra, se reconocen a menudo en otros documentos de políticas, no en uno de seguridad informática. Por eso, este manual atiende el punto de cómo mantener la información segura.

La teoría económica clásica sostiene que los activos y los recursos necesarios para hacer negocios son la tierra, la mano de obra y el capital. Otras teorías más recientes

La tabla de contenido de este manual ofrece solamente una lista de las políticas más relevantes, por ello es importante examinar todas las secciones para así encontrar las políticas que más se adapten a su área de interés. Por ejemplo, si sólo se leen las políticas que aparecen en la sección “[Seguridad Física y Ambiental](#)”, pueden dejar de verse otras importantes políticas que también tocan el área de la confidencialidad de los datos, pero que están en otras secciones.

Organización de las Políticas

Las políticas de este manual han sido organizadas de acuerdo con la Norma Internacional de Tecnología de la Información—Código de Prácticas para la Gestión de la Seguridad Informática, también conocida como ISO/IEC 17799. Esta jerarquía tiene la intención de permitir el fácil acceso a una gran cantidad de políticas asociadas a un tópico de interés. Este enfoque organizacional también permite la rápida identificación de las políticas relacionadas que puedan tener alguna conexión con el tópico o tema de interés.

Dentro de cualquier sección o de cualquier subsección, las políticas del manual no están organizadas de acuerdo con ninguna secuencia en particular. Esto significa que toda la sección debería revisarse cuando se está buscando alguna política en particular. Es importante revisar la Tabla de Contenido para identificar otras secciones que puedan también ser relevantes para el tema de interés.

dicen que los factores de producción son la gente, el dinero, la fábrica y los materiales. Pero a medida que nos insertamos más y más en la Era de la Información, debemos agregar a la información como otro factor de la producción. Un párrafo introductorio de este tipo debe servir para reforzar esta idea fundamental.

Otro objetivo motivacional tiene que ver con la responsabilidad fiduciaria de la gerencia en el sentido de conservar y proteger los activos y, como se dijo antes, la información ya se considera un activo. Esta perspectiva puede luego servir de fundamento para la creación de políticas explícitas en materia de seguridad informática. Esta tarea de la gerencia debería ser reconocida en el párrafo introductorio de la política de seguridad

informática. Para mayor información acerca del uso de estas ideas, ver el Capítulo 4, “[Modelo de Política de Seguridad Informática de Alto Nivel](#).”

Muchos enunciados de política hacen una breve presentación de lo que sucedería si no se prestara suficiente atención a la seguridad informática. Por ejemplo, muchos se refieren a la cantidad de riesgos que las políticas tienen la intención de atender. Desde el punto de vista legal, éstos incluyen el sabotaje, el terrorismo, el fraude y la estafa, la extorsión, el espionaje industrial, los errores y las omisiones, las interrupciones del servicio, el robo de equipos y la violación de la privacidad. Los riesgos también pueden evaluarse desde el punto de vista de negocio, cuando se habla de interrupciones de los negocios, decisiones gerenciales erróneas, desventaja competitiva, pérdida o destrucción de activos, mantenimiento impropio de registros y sanciones. Se recomienda que todos los enunciados de política hagan referencia a un conjunto de riesgos motivacionales, sin importar cómo se les caracterice.

Objetivos Operacionales

Las políticas deberían adecuarse a las circunstancias operacionales especiales de cada organización. Este proceso de adaptación puede empezar con políticas que estén enlazadas a los objetivos operacionales. Como ejemplo, el siguiente enunciado de objetivos puede ser utilizado para el conjunto de políticas de un manual de seguridad informática:

Este manual proporciona instrucciones definitivas de las políticas de seguridad informática que todos los trabajadores deben cumplir. Sus objetivos son:

- Familiarizar a los trabajadores con los riesgos en seguridad informática y las maneras que se espera sean atendidos dichos riesgos.
- Clarificar las responsabilidades y deberes del trabajador con respecto a la protección de los recursos informáticos.
- Facilitar la toma de decisiones por parte de la gerencia y otros trabajadores en materia de seguridad informática.
- Coordinar los esfuerzos de los distintos grupos de la Empresa X de manera de proteger de forma consistente los recursos informáticos, sin importar su ubicación, forma o plataforma tecnológica.
- Proporcionar orientación al proceso de auditoría de la seguridad de los sistemas informáticos y las evaluaciones de riesgo.

Alcance

El alcance de un documento de seguridad informática debería ser clarificado al inicio del proyecto de desarrollo de las políticas. La gerencia debería, por ejemplo, entender que este documento no se ocupará del protocolo formal. Los procesos disciplinarios deben ser parte de las políticas de Recursos Humanos, y no de un enunciado de política de seguridad informática. El control de calidad de la información y los tópicos de ingeniería tampoco deben formar parte del documento de políticas de seguridad informática. La seguridad física debe incluirse dentro del alcance del documento de políticas, pero sólo hasta donde arroje a la seguridad informática. Los tópicos de seguros y asuntos legales sólo deben cubrirse en términos de alto nivel en las políticas de seguridad informática.

Los documentos de política deben incluir enunciados específicos acerca de su aplicabilidad. Por ejemplo, un enunciado de política podría declarar que las políticas se aplican independientemente de:

- La manera en que se representa la información.
- La tecnología usada para manejar la información.
- La ubicación de la información
- La madurez de la información dentro de su ciclo de vida.

Los enunciados de política deben indicar quién debe respetar las políticas y cuándo es aceptable que las actuaciones o las actividades de los trabajadores no sean compatibles con las políticas. Por ejemplo, un enunciado podría establecer que las políticas deben ser respetadas por los empleados, el personal contratado, los consultores, los contratistas y los temporales, a menos que hayan recibido una autorización específica para hacer otra cosa, de parte del vicepresidente o de un gerente de mayor nivel. Este enfoque asume que hay un grupo centralizado de gerencia con suficiente autoridad para dictar políticas para toda la organización. Otra manera de ver la aplicabilidad de las políticas a individuos específicos sería la de exigir el acatamiento de la política por parte de los usuarios de los sistemas. Si continúan usando los sistemas de la Empresa X, los usuarios de manera implícita, y en algunos casos de manera explícita a través de la ventana de inicio de sesión, convienen en acatar las políticas de seguridad. Es recomendable ser muy específico acerca de las audiencias para las que se han escrito las políticas.

Escribir un documento de políticas de seguridad informática que se aplique a toda la organización en lugar de sólo a un segmento específico es la manera más eficiente y eficaz de proceder. Este enfoque logra consistencia y la aplicación total de los reglamentos definidos en el documento de políticas. Aunque esto sería lo ideal, en algunos casos este enfoque puede ser inconsistente con las estructuras organizacionales descentralizadas actuales. Tener un departamento centralizado de seguridad informática que genere las políticas para el resto de la organización es particularmente difícil si están involucradas filiales o empresas con varios socios. Si prevalece la estructura organizacional descentralizada, Seguridad Informática puede entonces emitir sugerencias que puede intentar vender como si fueran políticas a la gerencia de las otras unidades. En estos casos, el alcance de los enunciados de política podrían hacer referencia a la responsabilidad de la gestión de la seguridad informática en el sentido de proteger los activos informáticos, y ofrecer un conjunto de políticas como recomendación primera para la correcta protección de los activos informáticos.

Muchos enunciados de política de seguridad informática se han aplicado en el pasado sólo a la Tecnología Informática. Si bien este enfoque fue suficiente hace 10 años, los actuales sistemas de procesamiento distribuido requieren que las políticas de seguridad informática se apliquen a todos los usuarios del sistema dentro de la organización. Algunas organizaciones están expandiendo el alcance de sus esfuerzos en políticas de seguridad informática para incluir a los proveedores, clientes, y otros socios estratégicos. Esta definición tan amplia del alcance de las políticas de seguridad informática es producto de la inclusión en los nuevos sistemas de estos terceros como usuarios. Ejemplos de estos sistemas de amplio alcance incluyen los servicios de intercambio electrónico de datos, el correo electrónico, el comercio en Internet y las extranets.

Como principio, cada excepción que se otorga debilita la seguridad. Por ejemplo, si una organización adopta una política que exige que todos los trabajadores porten sus distintivos mientras estén en el área de computación, pero permite que los ejecutivos la ignoren, la política se verá notablemente disminuida. No sólo podrá causar esto que otros trabajadores se pregunten acerca del apoyo de la alta gerencia a la política, sino que hará que los visitantes pasen como dueños de casa porque los trabajadores simplemente supondrán que son ejecutivos. Aunque las estructuras organizacionales actuales, las políticas organizacionales y otros asuntos usualmente lo evitarán, el alcance de las políticas de seguridad informática debería incluir tantas unidades organizacionales, tipos de trabajadores y circunstancias como sea posible.

Debe haber consistencia entre el alcance de la responsabilidad del grupo de seguridad informática que está preparando las políticas y el alcance de las políticas propiamente dichas. Si el grupo responsable de la seguridad informática de una filial intenta redactar políticas para la casa matriz sin la aprobación previa de la gerencia, puede haber problemas. A menudo el alcance documentado de la responsabilidad de aquellos que preparan las políticas de seguridad informática tiene una definición más estrecha que el alcance de las políticas a preparar. Dado que se ha obtenido el apoyo de la gerencia para políticas muy amplias, ésta es una excelente oportunidad para que Seguridad Informática expanda su influencia y su responsabilidad formal.

Es importante definir con claridad el significado del término “seguridad informática”. Por su propia naturaleza, seguridad informática es multidisciplinaria, multidepartamental y crecientemente multiorganizacional. Las organizaciones tienen problemas para determinar a quién debe reportar seguridad informática

dentro de la organización, así como tienen dificultades para determinar el alcance del esfuerzo que deben hacer en seguridad informática. Una definición operativa recomendada para seguridad informática es “cualquier actividad que proteja la información y los sistemas informáticos”. Con esta definición, la información confidencial podría ser propiedad de un tercero y estar bajo la custodia de la organización, pero estaría dentro del alcance del esfuerzo de seguridad informática. Esta amplia definición incluye la información en papel y la información en formato de voz, no sólo la que pueda residir en computadores y redes. Es aconsejable argumentar esta amplia definición, aun cuando ya es suficientemente general, con la mención específica de las actividades desarrolladas por ciertos grupos internos, tales como planificación de contingencias, administración de sistemas, gestión de redes y gestión de registros. Otras actividades deben ser específicamente excluidas, tales como las de los grupos de auditorías tecnológicas, evaluaciones de riesgo, legales y seguridad física.

Otro factor relativo al alcance es el momento en que las políticas entran en vigencia. El documento de política debe claramente señalar el momento cuando los lectores pueden esperar la entrada en vigencia de las políticas. Algunas políticas muy específicas para situaciones van aún más allá, señalando cuándo expiran. Por ejemplo, si ciertas políticas de seguridad informática fueron adoptadas para facilitar el intercambio con un tercero, dichas políticas pueden expirar cuando termine el contrato con dicho tercero. En algunos casos, la fecha de emisión del documento de política precederá a la fecha de entrada en vigencia en por lo menos un par de meses, lo cual brinda una oportunidad a la gerencia para cambiar sus sistemas y así estar en cumplimiento. Algunas organizaciones reconocen el hecho de que frecuentes cambios en las políticas son necesarios y hasta esperados. Con este fin, las organizaciones pueden agregar palabras al final de sus documentos de política señalando que “la Empresa X se reserva el derecho de cambiar estas políticas en cualquier momento y sin previo aviso”.

Manejo del Incumplimiento

De acuerdo con las últimas investigaciones, el cumplimiento de las políticas de seguridad informática es inconsistente. Una encuesta reciente señala que sólo el 23% de más de 500 participantes dijeron que el cumplimiento era completo o casi completo. Al otro extremo, el 22% dijo que había poco o ningún cumplimiento. El incumplimiento es un problema serio

que destruye la utilidad de las políticas de seguridad informática. Por lo tanto, debe pensarse en maneras de manejar tanto el cumplimiento como el incumplimiento.

Después de redactadas las políticas, se debe notificar a los trabajadores que las políticas existen y que se espera su cumplimiento, aunque lo recomendable sería que también se hicieran programas y talleres de concientización al respecto para alcanzar el éxito del esfuerzo en materia de seguridad informática. Aunque está fuera del alcance de este manual, es bueno recordar que los proyectos de concientización y adiestramiento motivan a los trabajadores a tomar la seguridad informática en serio, venden los beneficios de los controles y logran su participación en la protección de los activos informáticos de la organización. Estudios muestran que si los trabajadores reciben adiestramiento inmediatamente después de la política, estarán más propensos a llevar a cabo sus tareas de manera consistente con el documento de política recién emitido. Un bosquejo de las distintas técnicas para transmitir estos mensajes se encuentra en el Apéndice D, “[Lista de Métodos Sugeridos para Aumentar Nivel de Conciencia](#).”

Siempre pasa que algunos piensan que esa política no es para ellos. Si ciertos gerentes creen que pueden estar en incumplimiento, es importante hacer que firmen un memo de aceptación de riesgos. Tales memos típicamente señalan que un gerente piensa que otras medidas de control que él toma son más que suficientes para compensar el control exigido en la política, o que está dispuesto a asumir el riesgo determinado por el incumplimiento. Dado que firmar este tipo de documentos tiene sus consecuencias, de carácter legal e intimidatorio, muchos gerentes prefieren cumplir antes que documentar su falta de cumplimiento. Además, intentar probar o defender la situación en incumplimiento, aceptando el memo de riesgo, puede ser muy difícil. Para una copia de un documento de aceptación de riesgo, ver Apéndice L, “[Declaración de Aceptación de Riesgo](#).”

El cumplimiento puede ser promovido a través de la obtención de firmas, bien sea desde el inicio del empleo o de manera periódica. Se recomienda que los receptores de las políticas de seguridad informática señalen por escrito que han leído, entendido y aprecian las implicaciones de las políticas. También se puede obtener la firma al momento de emitir un identificador de usuario o al renovar el mismo. Las firmas pueden enfatizar el hecho de que la gerencia toma la seguridad informática en serio y, además, proporcionan a la organización la evidencia escrita necesaria para justificar las medidas disciplinarias que se requieran, incluyendo el despido. Un ejemplo de este formulario

para la firma se encuentra en el Apéndice J, “[Convenio de Cumplimiento de las Políticas de Seguridad Informática](#).”

Excepciones de Responsabilidad

Necesidad de Adaptar

Las políticas aquí incluidas son genéricas y no deben utilizarse sin antes ser adaptadas al ambiente específico de seguridad de los sistemas informáticos de la organización. Para que tal adaptación sea la adecuada, deben satisfacerse los siguientes requisitos:

- Un especialista en seguridad informática debe estar presente e involucrado.
- El especialista debe poseer un amplio entendimiento de los riesgos que enfrenta la organización.
- El especialista debe entender los controles utilizados para manejar dichos riesgos.
- El especialista debe tener un buen entendimiento de las políticas existentes en materia de seguridad informática, así como de los lineamientos, los procedimientos, las normas y otros materiales.

Para que se cumplan estos requisitos, la organización que busque compilar un documento de seguridad informática necesitará realizar cierto trabajo de antecedentes. Por ejemplo, para el segundo requisito, se recomienda una evaluación de riesgo, tal como un análisis de escenarios, una evaluación de riesgo cuantitativa o una revisión de normas de diligencia debida. Para el cuarto requisito, considere completar una serie de entrevistas con las partes involucradas para entender no sólo lo que significan las políticas existentes, sino también cuán bien conocidas son las políticas, cuán bien los trabajadores las han cumplido, y los costos y beneficios que han generado las políticas actuales.

Equilibrios Necesarios

Dado que este manual contiene un conjunto completo de políticas, no debería sorprender a nadie el hecho de que algunas políticas aquí expuestas contradigan a otras de este mismo manual. Por ejemplo, las políticas relativas a la libertad de expresión pueden chocar con las políticas relativas a los derechos de privacidad. Cada organización tendrá que determinar dónde trazar los límites entre

unas y otras. Estas decisiones de la gerencia tienen que ser comunicadas a los trabajadores para evitar que las tomen ellos mismos, quizás con resultados catastróficos.

Como muchas otras actividades del mundo de la seguridad informática, la redacción de las políticas también exige sus equilibrios y el cambio de una cosa por otra. Entre los más comunes están los equilibrios entre costo y seguridad, velocidad y seguridad, flexibilidad y seguridad, y facilidad de uso y seguridad. Existen muchas condiciones y límites en el campo de la seguridad informática, por ello las políticas deben diseñarse de acuerdo con dichas condiciones y dichos límites. Por ejemplo, una política que tiene que ver con el despido de los empleados por violar ciertos requisitos de seguridad informática, puede ser incompatible con los convenios sindicales. Otros límites incluyen las prácticas normales de la industria, la cultura corporativa, la ética y moral de la sociedad, las leyes y los reglamentos, y la estructura de las relaciones con terceros.

Este manual pretende proporcionar una amplia variedad de políticas generalmente aceptadas. Pero eso no quiere decir que el cuerpo principal del manual está constituido por un conjunto de políticas consistentes desde el punto de vista lógico, aunque varias de éstas sí se encuentran al final de este manual. La inconsistencia lógica entre algunas políticas es también un reflejo del hecho de que no existe un conjunto normalizado de políticas específicas al que todas las organizaciones deban suscribirse, porque un conjunto lógico es aquel que ya está adaptado a las características específicas de cada organización.

Necesidad de Asesoramiento Competente

Muchas de las políticas descritas en este manual contienen números específicos, períodos de tiempo u otra información que depende o bien de tecnología, o bien de la jurisdicción o bien de una organización. Por consiguiente, se recomienda emplear los servicios de un buen abogado, entendido en las artes computacionales, y los de un buen especialista en seguridad informática, antes de sacar a la luz pública estas políticas, o sus derivados. En algunos casos, como cuando se instauran políticas de cifrado, puede ser aconsejable obtener la ayuda de un especialista en un área muy específica.

También se recomienda la revisión el director de Recursos Humanos para evitar conflictos con las políticas actuales de la organización.

Por último, el material de este manual tiene el propósito de proporcionar orientación e ideas para la generación de políticas potenciales. Su intención no es la de ofrecer un curso específico de acción o un conjunto específico

de palabras para una organización. Algunas de las sugerencias de este manual pueden tener poca o ninguna importancia para ciertas organizaciones, y pueden ser hasta ilegales en algunas jurisdicciones. El material de este manual no debe ser usado textualmente, sino que debe adaptarse a las circunstancias específicas de cada organización.



Capítulo 3 POLÍTICAS ESPECÍFICAS

3 POLÍTICA DE SEGURIDAD

3.01 Política de Seguridad Informática

3.01.01 Documento de Políticas de Seguridad Informática

1. Protección de la Información

Política: La información debe ser protegida de acuerdo con su confidencialidad, valor y criticidad.

Comentario: Esta política se aplica sin importar el medio o ubicación donde esté guardada la información, los sistemas tecnológicos utilizados para procesarla, o las personas que la manejen. Esta política promueve la revisión de las formas en que la información fluye a través de una organización y, además, indica el alcance del trabajo de la gerencia de Seguridad Informática dentro y fuera de la organización. La política conlleva a Auditoría Interna a emplear técnicas integradas tales como el análisis de flujo de datos. La idea que da origen a esta política es importante para aquellos que preparan una arquitectura de sistemas de seguridad. Los sistemas integrados de control de acceso que utilizan esta idea podrían incluir la conexión individual a una red de computadores, un lugar único para el registro de usuarios, la administración centralizada del control de acceso y la auditoría centralizada del sistema de control de acceso. En algunos casos se pueden suministrar ejemplos específicos para aclarar esta política.

Políticas Relacionadas: “Mecanismo Único de Acceso,” “Normas de Implementación de Controles,” “Comité de Gestión de Seguridad Informática,” y “Dispersión de Sistemas Computacionales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Uso de la Información

Política: La información de la Empresa X debe ser usada únicamente para los propósitos de negocios expresamente autorizados por la gerencia.

Comentario: Esta política establece que están prohibidos todos los usos no autorizados de la información de la Empresa X. Por ejemplo, un empleado puede desear utilizar la base de datos de clientes de su empleador para hacer envíos masivos de correo con fines caritativos. Esta política puede aplicarse en toda instancia o escribirse únicamente en la etiqueta de los medios de almacenamiento de información susceptibles de abuso, tales como las listas de correo de clientes. Para evitar los problemas de difusión secundaria es altamente recomendable el marcaje de la información confidencial. Esta política es importante para todos los trabajadores que estén en contacto con la información de la Empresa X. En esta política, el enfoque radica más en el uso de la información que en los sistemas que la manejan.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Uso Distinto al Empresarial de la Información de la Organización,” y “Manejo de Información Sensible”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Manejo, Acceso y Uso de la Información

Política: La información es un activo vital y todos los accesos, usos y manejos de la información de la Empresa X deben ser consistentes con sus políticas y normas.

Comentario: Esta política establece el contexto para muchas otras políticas de seguridad informática. Tal afirmación es frecuentemente incorporada al primer conjunto de políticas y resúmenes que se dirige a los usuarios y a los integrantes de la alta gerencia. Es necesario que estas personas comprendan cómo la información se ha convertido en un factor crucial para la producción empresarial. Esta política determina la necesidad de establecer medidas de seguridad

informática y de crear una nueva comprensión de la importancia de los sistemas informáticos en las organizaciones.

Políticas Relacionadas: “Uso Distinto al Empresarial de la Información de la Organización”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

4. Excepciones de Responsabilidad por Daños a Datos y Programas

Política: La Empresa X no se hace responsable por pérdidas o daños a datos o software, que provengan de su esfuerzo por proteger la confidencialidad, integridad y disponibilidad de la información manejada por los computadores y los sistemas de comunicación.

Comentario: Esta política informa al usuario que no puede responsabilizar a la Empresa X por daños causados por los intentos de la gerencia de asegurar su sistema. Por ejemplo, si el administrador del sistema se encuentra realizando una exploración rutinaria anti-virus en todos los computadores de una red local, lo que parezca ser un virus se detectaría y se ejecutaría un programa de erradicación de virus. Esta acción puede alterar el programa infectado e inutilizarlo. Cuando el usuario determina que el programa es inoperante, no puede culpar a la gerencia de haberlo dañarlo. Esta política se aplica más efectivamente en lugares donde la Empresa X posee instalaciones utilizadas por gente distinta a sus empleados, como es el caso de las universidades donde los usuarios son estudiantes.

Políticas Relacionadas: “Privilegios Especiales en Sistema” y “Sin Responsabilidad en Mensajes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

5. Conflictos Legales

Política: Las políticas de seguridad informática de la Empresa X han sido diseñadas de tal manera que cumplan o excedan las protecciones derivadas de las leyes y los reglamentos existentes y cualquier política de seguridad informática de la Empresa X que se suponga en conflicto con dichas leyes o regulaciones debe ser reportada inmediatamente a la gerencia de Seguridad Informática.

Comentario: Esta política crea la base de los requisitos especificados en un documento de políticas de seguridad informática. Las políticas apropiadas van más allá de las leyes y los reglamentos, o al menos garantizan que una organización cumplirá los requisitos especificados en dichos reglamentos y leyes. Esta política reconoce su apoyo a las leyes y los reglamentos, y expresa la intención de siempre cumplir las leyes y los reglamentos existentes. Esta política es conveniente tanto para las políticas de seguridad informática internas como para aquellas disponibles al público.

Políticas Relacionadas: “Informes de Incidentes” y “Propiedad de Archivos y Mensajes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

6. Excepciones a las Políticas

Política: Se dan excepciones a las políticas de seguridad informática en las raras ocasiones en que se ha producido una evaluación de riesgo de las implicaciones de no cumplir las políticas, preparándose entonces un formulario normalizado de aceptación de riesgo por parte del Propietario de los datos o la gerencia, siendo dicho formulario aprobado tanto por la gerencia de Seguridad Informática como por la de Auditoría Interna.

Comentario: La gerencia será la llamada a autorizar las pocas excepciones a las políticas. Esta política aclara que las excepciones serán otorgadas únicamente después de completar, firmar y autorizar un formulario de aceptación de riesgos. Este formulario debe incluir una declaración en la cual el Propietario de los datos o la gerencia asumen la responsabilidad por cualquier pérdida ocurrida durante el período de incumplimiento de las políticas. La existencia de dicho formulario facilita una válvula de escape que puede ser utilizada para las situaciones en las cuales los usuarios insisten en el incumplimiento de las políticas. Es deseable lograr que todos los desacuerdos sean conocidos y documentados. Esto significa que si ocurre una pérdida como resultado de dicha situación, la gerencia puede demostrar ante un juez o jurado que estaba en conocimiento de la situación, estudió los riesgos y decidió renunciar a la política o norma habitual.

Políticas Relacionadas: “Consecuencias de Incumplimiento,” “Renuncia a Derechos de Privacidad,” y “Cumplimiento Forzoso de los Controles de Seguridad”

Política Dirigida a: Gerencia

Ambientes de Seguridad:Todos**7. Sin Obligación de Hacer Cumplir las Políticas**

Política: El hecho de que la gerencia no haga cumplir algún requerimiento de las políticas no significa que otorga su consentimiento.

Comentario: A través de esta política se hace del conocimiento de aquellos que la lean que no deben suponer la continuación de las condiciones de incumplimiento sólo porque la gerencia aún no haya exigido su cumplimiento. Esta política elimina cualquier reclamo que la gerencia local haga respecto a que una condición de incumplimiento debe permanecer como está porque dicha condición existe desde hace ya cierto tiempo.

Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno” y “Mensaje de Inicio de Sesión en la Red”

Política Dirigida a: Usuarios finales**Ambientes de Seguridad:**Todos**8. Infracción de la Ley**

Política: La gerencia de la Empresa X debe considerar seriamente el enjuiciamiento de toda infracción conocida de las leyes.

Comentario: Esta política promueve el enjuiciamiento de actos abusivos y criminales. Si bien la decisión de enjuiciar dependerá de lo específico del caso, la gerencia no debería descartar el enjuiciamiento sin realizar una revisión. Esta política puede resultar importante si se comunica a los potenciales autores de actos abusivos y criminales. Numerosos crímenes informáticos no son enjuiciados y los autores están conscientes de ello, suponiendo que las organizaciones víctimas de dichos crímenes sólo los despedirán y ocultarán lo ocurrido. Una política como ésta es utilizada, por ejemplo, por varias compañías de teléfono con aquellos individuos que obtienen servicios telefónicos de manera fraudulenta. En vez de estar establecida en términos generales, esta política podría requerir el enjuiciamiento de ciertos crímenes que ocurren normalmente en el ámbito del negocio involucrado, tal como lo es el fraude con las tarjetas de crédito.

Políticas Relacionadas: “Informes de Incidentes”

Política Dirigida a: Gerencia**Ambientes de Seguridad:**Todos**9. Revocación de Privilegios de Acceso**

Política: La Empresa X se reserva el derecho de revocar los privilegios sobre tecnología informática al usuario en cualquier momento.

Comentario: Esta política informa a los usuarios que ponen en peligro su calificación como usuarios autorizados si se involucran en actividades que interfieren con la operación normal y propia de los sistemas informáticos de la Empresa X, que afecten negativamente la habilidad de otros para utilizar dichos sistemas informáticos o que son dañinas u ofensivas a otros. Por ejemplo, colapsar el sistema podría ser dañino para otros usuarios y el autor estaría sujeto a acciones disciplinarias en su contra, incluyendo la revocación de privilegios. La política intenta describir ampliamente una ética en computación. En vez de especificar todas las cosas negativas que la gente podría hacer, como colapsar un sistema, esta política es discreta y se ubica en un nivel alto. Esta política puede dar espacio a la gerencia al momento de decidir sobre la revocación de privilegios.

Políticas Relacionadas: “Privilegios Predeterminados de Usuario” y “Reautorización de los Privilegios de Acceso de Usuario”

Política Dirigida a: Usuarios finales**Ambientes de Seguridad:**Todos**10. Normas de Seguridad Informática Específicas a Cada Industria**

Política: Los sistemas informáticos de la Empresa X deben regirse por normas de seguridad informática específicas a cada tipo de industria.

Comentario: Esta política requiere que los diseñadores de sistemas y el personal técnico utilicen controles que satisfagan las normas de cada industria. Por ejemplo, en la banca, los sistemas de criptografía deben utilizar sistemas específicos a la industria bancaria para el manejo de las claves. Otros controles específicos son importantes para la industria de servicios médicos, la comunidad aeroespacial y de defensa y otros grupos industriales.

Políticas Relacionadas: “Compra de Soluciones de Seguridad Informática,” “Normas de Implementación de Controles,” y “Controles Mínimos en Sistemas Informáticos”

Política Dirigida a: Personal técnico**Ambientes de Seguridad:**Todos

11. Uso de Políticas y Procedimientos de Seguridad Informática

Política: Toda la documentación referente a la Seguridad Informática de la Empresa X, inclusive, sin limitación, de las políticas, normas y procedimientos, debe ser clasificada como "Sólo Para Uso Interno", a menos que haya sido expresamente creada para ser utilizada para procesos de negocios externos o por socios.

Comentario: Esta política evita que los trabajadores revelen a terceros los detalles de cómo la Empresa X asegura su información y sus sistemas, ya que pueden ser utilizados para comprometer la información y los sistemas de la Empresa X. Por ejemplo, el conocimiento de los procesos internos podría ayudar a un espía industrial a cometer un fraude creíble de ingeniería social. Debido a que algunas políticas de Seguridad Informática son dadas a conocer al público, algunos trabajadores podrían tener la impresión de que otras

políticas también podrían ser dadas a conocer al público sin problema. Pero debe enfatizarse que las políticas referentes a la Seguridad Informática pueden ser reveladas a terceros sólo cuando lo exijan razones empresariales o porque es lo correcto. No todas las políticas de seguridad informática deben ser reveladas en estos casos y una declaración breve no es sólo recomendable sino también apreciada por las personas que la reciben. Cada documento sobre una política referente a la seguridad informática debe ser marcado mediante una clasificación apropiada para así enfatizar el hecho de que las políticas no constituyen información de dominio público.

Políticas Relacionadas: “Convenio de Trabajo” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3.01.02 Revisión y Evaluación

1. Cumplimiento Forzoso de los Controles de Seguridad

Política: Todos los sistemas de control de la seguridad informática deben ser susceptibles de cumplimiento forzoso antes de adoptarse como parte normal del proceso operativo.

Comentario: Los controles que no son de cumplimiento forzoso tienden a hacerse inservibles. Por ejemplo, si la gerencia tiene una política acerca de escritorios vacíos, que consiste en guardar bajo llave todo el material confidencial después del trabajo, y no se obliga a su cumplimiento, los empleados rápidamente aprenden a ignorar dicha política. Es intencional que esta política requiera que la gerencia revise el cumplimiento forzoso de los controles, lo cual es un asunto que puede no ocurrir antes de adoptar un control. Por ejemplo, la gerencia puede adoptar una política que exija la revisión de los registros de control de acceso para detectar actividades no autorizadas, pero después de haberla adoptado, la gerencia podría darse cuenta de que requiere demasiado tiempo por parte del personal. Por eso, puede ser recomendable tener una definición previa

del concepto de "cumplimiento forzoso" en algunos casos. Para que un control se cumpla debe ser posible para la gerencia determinar claramente si el personal cumple y si el control está logrando el objetivo para el cual fue diseñado. La política es intencionalmente imprecisa sobre lo que constituye el procedimiento operativo normal. Esto permite que la política sea aplicable a una amplia variedad de circunstancias sin importar si el control es documentado, específico a un departamento o utilizado de manera experimental. En algunos casos esta política puede requerir que los diseñadores de los controles añadan un mecanismo de monitoreo que reporte el status del control. Por ejemplo, las cajas de cifrado de algunos proveedores tienen luces que indican que están funcionando en la forma en que deben hacerlo.

Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno” y “Convenios con Terceros”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4 SEGURIDAD ORGANIZACIONAL

4.01 Infraestructura de la Seguridad Informática

4.01.01 Foro Gerencial Sobre Seguridad Informática

1. Alteración No Detectada de la Información

Política: La gerencia debe establecer y mantener las medidas de seguridad, prevención y detección necesarias para garantizar que la información de la Empresa X está protegida del riesgo de alteraciones no detectadas.

Comentario: Esta política orienta a los diseñadores de sistemas, especialistas en redes y otros, en la implantación de las medidas de control adecuadas para prevenir las alteraciones de la información no detectadas. La naturaleza exacta de estos controles varía considerablemente de sistema a sistema. Esta política señala que es importante detectar todas las modificaciones no autorizadas y que las mismas deben prevenirse siempre que sea posible, e implica, además, que todos los cambios de la información deben tener un rastro auditble, de tal forma que el motivo de las modificaciones efectuadas y la persona que los realiza puedan ser identificado. Los controles utilizados para lograr esta política son de diferentes formas, tales como firmas digitales, códigos de autentificación de mensajes, mensajes cifrados y certificados digitales. Una política como ésta es especialmente importante para organizaciones de servicios en la industria financiera, pues es perfecta para definir controles anti-fraude y anti-malversación. Algunas organizaciones la pueden modificar para restringirla sólo a la información sensible, valiosa y crítica para la empresa. Estas modificaciones pueden ahorrar dinero, puesto que previenen la asignación innecesaria de recursos para proteger datos que no son sensibles ni críticos.

Políticas Relacionadas: “Identificación de Requisitos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Comité de Gestión de Seguridad Informática

Política: Un comité gerencial de seguridad informática, compuesto por la alta gerencia o sus delegados de cada división principal de la Empresa X, debe reunirse

trimestralmente para revisar el nivel actual de seguridad informática, revisar los procesos de monitoreo de los incidentes de seguridad de la Empresa, aprobar y luego revisar los proyectos de seguridad informática, aprobar políticas nuevas o modificadas de seguridad informática y realizar otras actividades gerenciales de alto nivel necesarias para mantener la seguridad informática.

Comentario: Los objetivos de esta política consisten en proporcionar una misión a un comité gerencial de nivel medio en el tema de la seguridad informática, además de señalar lo que se espera de dicho comité. Algunas organizaciones poseen un comité permanente mientras otras lo tienen temporal. Los comités temporales existen para brindar suficiente apoyo a un proyecto de seguridad informática hasta que se mantenga a sí mismo sin ayuda del comité. Los objetivos específicos del comité pueden modificarse para satisfacer las necesidades organizacionales. Otros objetivos de esta política incluyen definir roles y responsabilidades específicos en la medida en que se refieran a seguridad informática, a autorizar el uso de metodologías y procesos específicos de seguridad informática, a garantizar que ésta se integre a los otros procesos de planificación y control de cambios de la Empresa X, a coordinar la implantación de las medidas de seguridad informática específicas correspondientes y a promover la visibilidad de la seguridad informática dentro de la empresa. En los objetivos no se harán referencias detalladas de las actividades, puesto que el trabajo del comité está restringido a políticas y asuntos de alto nivel. De igual manera las actividades pormenorizadas cambian sustancialmente con el tiempo y esta política debe ser escrita para que prevalezca durante varios años. Comités como estos sirven para incrementar la concientización gerencial sobre la seguridad informática y lograrla de manera consistente a lo largo de grandes organizaciones con diversas culturas y procesos de trabajo.

Políticas Relacionadas: “Seguridad Informática Centralizada” y “Revisión del Impacto Sobre la Privacidad”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4.01.02 Coordinación de Seguridad Informática

1. Riesgos Significativos para la Seguridad Informática

Política: Por cada riesgo importante para la seguridad de los sistemas informáticos, la gerencia debe tomar una decisión específica acerca del extremo al que está dispuesta a llegar la Empresa X para aplicar su propio seguro y aceptar el riesgo, buscar cobertura externa o ajustar los controles para reducir las pérdidas.

Comentario: Esta política requiere que la gerencia, particularmente aquellos que actúan como Propietarios de la información, respondan a los hallazgos de los auditores o terceros de las vulnerabilidades existentes en materia de seguridad. La gerencia a menudo ignora la situación, convirtiéndose en su propia aseguradora sin entender las razones que la empujan a tomar dicha decisión. Para garantizar que se haga lo correcto, algunas organizaciones pueden optar por incluir las palabras "por escrito" en la política. Esta política puede ser cambiada para notificarle a la gerencia que se dispone de un seguro para abordar algunos de estos problemas, aún cuando la decisión principal está en escoger entre invertir en los controles o aceptar el riesgo.

Políticas Relacionadas: ["Normas de Implantación de Controles"](#) y ["Evaluación del Riesgo en los Sistemas de Producción"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Cobertura de Seguros

Política: Se debe obtener una cobertura de seguro adecuada y vigente para cada amenaza significativa a la confidencialidad, integridad y disponibilidad de la información manejada a través de los sistemas de computadores y de comunicaciones de la Empresa X.

Comentario: Esta política requiere que la gerencia investigue las necesidades de cobertura de la organización, particularmente en lo referente a la confidencialidad, integridad y disponibilidad de la información. La política requiere, además, que la cobertura de seguro se mantenga vigente. La gerencia debe cuantificar el riesgo financiero y determinar cuánta cobertura es necesaria. Para ciertos tipos de cobertura esto también significa que los requerimientos de la aseguradora deben ser respetados por la empresa asegurada. Esta política informa que dicho seguro existe, lo que ciertamente puede resultar novedoso para algunos integrantes del equipo gerencial. Esta política no requiere tomar acción alguna por amenazas insignificantes. Esta política es especialmente importante para todas aquellas industrias en las cuales la información es o se está convirtiendo en la esencia de sus negocios.

Políticas Relacionadas: ["Evaluación del Riesgo en los Sistemas de Producción,"](#) ["Directorio de Almacenamiento de Archivos,"](#) y ["Fianzas de Trabajadores"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4.01.03 Asignación de Responsabilidades en Seguridad Informática

1. Propiedad de la Información

Política: El jefe principal de la seguridad informática debe claramente especificar, por escrito, la asignación de las responsabilidades de la propiedad de la información para las bases de datos, los archivos maestros y otras recopilaciones de información compartidas y debe designar a las personas con derecho a acceder a dichas recopilaciones en nombre de los Propietarios.

Comentario: Esta política establece la delegación clara y documentada de la autoridad para ejercer el control del acceso a la información. Una definición de las autoridades delegadas es útil para establecer los

permisos al control del acceso. Esta política clarifica quién es responsable de la seguridad y lo correspondiente a los recursos informáticos compartidos, tales como una base de datos o una partición de archivos en red. A menudo, las actividades de seguridad informática se olvidan cuando varias personas son potencialmente responsables, pero a ninguna se ha asignado la responsabilidad como tal. Esta política es útil dentro de organizaciones que dependen de un sistema administrativo de base de datos y aplicaciones de programas que imponen controles de acceso. A menudo no queda claro que los administradores de la base de datos y el personal técnico de soporte de sistemas son los responsables de administrar los controles de acceso a los sistemas. El

proceso para designar quién es responsable del control de acceso permitirá encontrar los sitios donde falta designar a un responsable.

Políticas Relacionadas: “[Asignación de la Propiedad de la Información](#)” y “[Transferencia de Responsabilidad en Custodia](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Cambios en Situación del Trabajador

Política: Toda modificación en la condición laboral de los trabajadores de la Empresa X, inclusive, sin limitantes, de los asesores, contratistas y temporales, debe ser reportada inmediatamente por la gerencia a Recursos Humanos, quienes a su vez deben notificar a los administradores de los sistemas informáticos correspondientes.

Comentario: La intención de esta política es establecer una conexión entre la base de datos de Recursos Humanos y la base de datos del control del acceso que supervisan los administradores del sistema informático. Las empresas deben recordar a la gerencia de la unidad de negocios que ella es responsable de mantener una vía de comunicación transparente con Recursos Humanos con respecto a las condiciones de su personal. En muchas ocasiones, los administradores de sistemas, y algunas veces Recursos Humanos, no están en conocimiento de las transferencias, jubilaciones, permisos y otros cambios parecidos en la condición de los trabajadores. Los Administradores no hacen los cambios necesarios en los privilegios de control de acceso de estos trabajadores y no hacer estos cambios a tiempo puede resultar en fugas de información confidencial o en sabotaje del sistema. Aunque la política no habla específicamente de una conexión automatizada, ésta es conveniente en cualquier organización que tenga 100 o más trabajadores. Esta política es especialmente eficaz en las organizaciones que cuentan con un sistema empresarial de gestión de la seguridad que usualmente dependa de una base de datos centralizada de privilegios de usuario a lo largo de todos los sistemas operativos y máquinas propias específicas. Esta política puede implementarse de manera manual, pero con mayor probabilidad de errores y retardos. Si la gerencia puede emplear, despedir o contratar personas sin involucrar o notificar a Recursos Humanos, entonces esta política podría cambiarse para exigir a la gerencia local reportar dichos cambios a los administradores del sistema.

Políticas Relacionadas: “[Informe de Cambios en Situación de Empleados](#)” y “[Reautorización de los Privilegios de Acceso de Usuario](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Enfoque Gerencial de la Seguridad

Política: La gerencia debe garantizar que la seguridad informática dentro de cada departamento sea tratada como un problema empresarial normal a ser afrontado y resuelto, siendo la misma gerencia responsable de promover la seguridad como problema de todos.

Comentario: Esta política confronta a la gerencia con su propia actitud y le permite darse cuenta que debe sentar un ejemplo para los trabajadores de su departamento. En muchas organizaciones, la gerencia se opone a la seguridad informática y ha impedido su progreso. Esta política ayuda a la gerencia a reconocer la seguridad informática como función empresarial. También resalta el hecho de que la seguridad informática no es un proyecto que pueda ser completado y luego olvidado, sino que es una operación empresarial continua que debe ser apoyada.

Políticas Relacionadas: “[Convenio de Trabajo](#)” y “[Planes de Recuperación Ante Desastre Computacional](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4. Evaluaciones de Riesgos

Política: La evaluación de los riesgos en seguridad informática debe ser realizada por terceros no interesados.

Comentario: Esta política evita que el personal interno revise su propio trabajo. Durante el proceso de trabajo, el personal interno puede no detectar fallas importantes que aparecerán sólo cuando se produzca un incidente. Debido a que la seguridad informática es tan compleja, debe ser revisada frecuentemente por un tercero, preferiblemente por un experto en el área correspondiente. Por ejemplo, si se va a realizar una evaluación de riesgo en el control de acceso a la red, éste debe ser hecho por alguien con experiencia en esa área, no en un área relacionada, como los virus de computadores. Con esto presente, la palabra “experto” debe ser añadida a la política. La gerencia frecuentemente no se da cuenta de que la gente que realiza las revisiones de seguridad

carece de independencia, y esto se observa cuando los vendedores ofrecen revisiones de seguridad como regalo o a bajo costo para luego recomendar que la organización adopte las soluciones que ellos plantean a los problemas que ellos mismos encontraron.

Políticas Relacionadas: “Evaluaciones de Riesgo de los Sistemas” y “Evaluación de Nuevas Tecnologías”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

5. Productos y Servicios de Seguridad

Política: Toda función crítica de seguridad informática debe estar apoyada con lo mejor de lo mejor en productos y servicios comerciales disponibles en el mercado.

Comentario: Esta política expresa una filosofía de diseño de sistemas seguros y especifica cómo debe ser implementada desde el punto de vista empresarial. Se pretende mediante esta política garantizar que todos los productos de seguridad informática importantes y los servicios correspondientes, estén respaldados por las mejores soluciones comerciales disponibles. Se señalan explícitamente soluciones comerciales puesto que las no comerciales pueden no estar respaldadas o no mantenerse actualizadas. El personal de seguridad informática habitualmente determinaría cuáles funciones son críticas y cuáles deben estar respaldadas por las mejores soluciones. Esta política requiere que el personal interno realice investigaciones adicionales para comprender lo que ofrece el mercado actual.

Políticas Relacionadas: “Madurez del Producto de Seguridad” y “Compra de Soluciones de Seguridad Informática”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Alto

6. Recursos para la Seguridad Informática

Política: La gerencia debe suministrar suficientes recursos y atención al personal para poder ocuparse adecuadamente de la seguridad de los sistemas informáticos.

Comentario: Esta política señala a la gerencia de bajo nivel que la seguridad informática es importante y no puede ser ignorada. Es particularmente apropiada para organizaciones descentralizadas, tales como una casa matriz con filiales. Esta política también separa una

partida presupuestaria para la protección de la información y los sistemas de la Empresa X. La palabra "suficientes" es deliberadamente ambigua. La política implica que se debe hacer una evaluación del riesgo y puede ser muy útil en aquellas organizaciones que emplean sistemas contables de reversión de cargos por servicios computacionales y de telecomunicaciones. Esta reversión de cargos a menudo desanima a los usuarios de utilizar estos servicios para atender asuntos relativos a la seguridad informática.

Políticas Relacionadas: “Evaluación del Riesgo en los Sistemas de Producción” y “Controles Mínimos en Sistemas Informáticos”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

7. Partida Presupuestaria para la Seguridad Informática

Política: Los productos y servicios de seguridad informática deben cargarse a los presupuestos de gastos corporativos y no deben revertirse a cada filial.

Comentario: Esta política promueve la asignación de fondos suficientes para la seguridad informática en las grandes organizaciones que poseen divisiones, filiales u otro tipo de unidades organizacionales. Cuando se utilizan sistemas de reversión de cargos para transferir los costos por seguridad informática, la gerencia de la unidad afectada a menudo decide reducirla o eliminarla. Esto no representa problemas serios si cada unidad posee sistemas informáticos independientes y desconectados, pero si están conectados a través de una red, se requiere uniformidad para lograr un nivel adecuado de seguridad. Al presentarse un presupuesto central único, mejora ampliamente el cumplimiento de las normas internas de seguridad informática. Las unidades organizacionales separadas pueden escoger métodos propios o autorizaciones especiales. Esta política garantiza que todas las unidades tengan suficientes controles, sin importar su presupuesto o su reciente producción financiera. Esta política aborda uno de los problemas de diseño organizacional que a menudo reducen la seguridad informática a posiciones de irrelevancia o ineficacia.

Políticas Relacionadas: “Recursos para la Seguridad Informática” y “Facturas por Servicios Computacionales y Comunicacionales”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

8. Autorización para Cambios de los Sistemas Informáticos

Política: Los gerentes de departamento u otros integrantes del equipo gerencial no pueden firmar contratos, iniciar proyectos internos ni de otra manera comprometer a la Empresa X a efectuar modificaciones en sus sistemas de computación o de comunicación, a menos que tales modificaciones hayan sido autorizadas previamente tanto por el jefe principal de información como por la gerencia de Seguridad Informática.

Comentario: Esta política notifica a la gerencia interna que no debe comprometerse a hacer modificaciones en los sistemas computacionales o de comunicaciones sin la autorización del jefe principal de información y la de la gerencia de Seguridad Informática. Sin una política como ésta, la gerencia puede hacer promesas, a menudo a contratistas o asesores, que luego derivan en serios problemas de seguridad. Aun cuando esta política no tenga suficiente fuerza legal como para rescindir un contrato, su propósito es que la gerencia interna consulte con el jefe principal de información y la gerencia de Seguridad Informática antes de hacer promesa alguna.

Políticas Relacionadas: “[Procura de Hardware y Software](#)” y “[Correo Electrónico del Departamento de Ventas](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

9. Seguridad Informática Centralizada

Política: La orientación, dirección y autoridad de las actividades de seguridad informática están centralizadas para toda la organización en la Gerencia de Seguridad Informática.

Comentario: Esta política indica claramente a todos los trabajadores que la gerencia de Seguridad Informática está a cargo de cualquier asunto relacionado con la seguridad informática. Muchas organizaciones mantienen discusiones internas sobre quién tiene la responsabilidad final de la Seguridad Informática. Esta área es particularmente problemática con redes de área local, computadores personales, sistemas cliente-servidor y otros sistemas menores que han sido controlados casi totalmente por los departamentos usuarios, en lugar de un departamento centralizado de Sistemas Informáticos. Esta política no implica que todo el trabajo de seguridad informática será realizado por Seguridad Informática. Deben existir coordinadores departamentales, administradores de seguridad local y otros encargados específicamente del trabajo de

seguridad informática. Para ser eficaces en la era de redes integradas, de políticas de seguridad informática, las normas, las arquitecturas y los asuntos de infraestructura correspondientes, deben ser dictados de manera centralizada por un grupo de seguridad informática que abarque toda la organización.

Políticas Relacionadas: “[Comité de Gestión de Seguridad Informática](#),” “[Convenciones en Desarrollo de Sistemas](#),” “[Solicitudes de Información Organizacional](#),” “[Cambios en la Línea de Comunicación](#),” “[Procura de Hardware y Software](#),” y “[Punto Central de Falla de la Red](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Responsabilidades del Departamento de Seguridad Informática

Política: El departamento de Seguridad informática es responsable de establecer y mantener las políticas, normas, lineamientos y procedimientos relativos a la seguridad informática de toda la organización.

Comentario: Uno de los propósitos de esta política es aclarar que el departamento de Seguridad Informática tiene responsabilidades que abarcan toda la organización. Otro propósito es enfatizar que el enfoque de Seguridad Informática es la información, no los computadores. Aunque desde el punto de vista organizacional dependa del jefe principal de información de una filial importante o del director del departamento de Tecnología Informática, Seguridad Informática debe ser vista como la autoridad a lo largo de toda la organización. Esta política comunica a los trabajadores la función y el trabajo de Seguridad Informática. Muchos trabajadores tienen la noción de que Seguridad Informática se ocupa de todo lo relacionado con la seguridad de la información y que ellos no necesitan involucrarse. Por ello, las tareas delineadas en la política deben ser modificadas para reflejar el diseño y la estructura organizacional de la Empresa X. Por ejemplo, esta política podría incluir investigaciones, revisiones del cumplimiento y otras actividades. Algunas organizaciones preferirían colocar el material de esta política en su declaración de misión o en sus estatutos, pero no como política.

Políticas Relacionadas: “[Seguridad Informática Centralizada](#),” “[Responsabilidad en la Seguridad Informática](#),” “[Misión del Departamento de Seguridad Informática](#),” y “[Tareas del Departamento de Seguridad Informática](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

11. Tareas del Departamento de Seguridad Informática

Política: La gerencia de Seguridad Informática debe proporcionar dirección y pericia técnica para garantizar que la información de la Empresa X está protegida con procesos que mantienen la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas que la manejan.

Comentario: Esta política proporciona información específica sobre las responsabilidades del departamento de Seguridad Informática. Este departamento debe realizar varias tareas incluyendo, sin limitantes, evaluar riesgos, preparar planes de acción, evaluar los proveedores de productos, participar en proyectos de desarrollo de sistemas internos, ayudar con la implementación de los controles, investigar las brechas de seguridad informática y adiestrar a otros miembros del personal. Muchos trabajadores no entenderán las obligaciones y las contribuciones aportadas por Seguridad Informática. Por eso, esta política puede eliminar la incertidumbre y enfocar el trabajo del departamento. La política define la seguridad informática en un sentido amplio para incluir toda la información plasmada en papel, en voz, en gráficos hechos a mano, la contenida en productos y otras manifestaciones de la misma.

Políticas Relacionadas:[“Responsabilidades del Departamento de Seguridad Informática”](#)

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

12. Misión del Departamento de Seguridad Informática

Política: El departamento de Seguridad Informática es responsable de evitar perder o comprometer los recursos informáticos críticos, valiosos y sensibles de la Empresa X, a través de la coordinación y direccionamiento de acciones específicas que proporcionen un ambiente informático seguro y estable, consistente con las metas y objetivos de la Empresa X.

Comentario: Esta política apoya las metas y objetivos de la Empresa X. La Seguridad Informática a menudo se percibe como un obstáculo o estorbo para las metas y

objetivos de la Empresa X. Esta afirmación trata de minimizar declaraciones sobre sucesos negativos. Esta caracterización positiva de la Seguridad Informática fomenta la visión de contribuir, en vez de inhibir, al crecimiento y la expansión. La declaración de la misión pretende claramente apoyar las metas y objetivos de la Empresa X. Algunas organizaciones querrán ser más específicas en la manera en que el departamento apoya las metas y objetivos de la organización.

Políticas Relacionadas:[“Responsabilidades del Departamento de Seguridad Informática”](#)

Política Dirigida a:Gerencia y personal técnico

13. Normas y Procedimientos de Seguridad Informática

Política: El departamento de Seguridad Informática tiene la autoridad para crear y periódicamente modificar las normas técnicas y los procedimientos operativos que apoyan a estos datos documentales de la política de Seguridad Informática, los cuales, al ser aprobados por la gerencia correspondiente de la Empresa X, tendrán el mismo alcance y autoridad que tendrían si estuvieran incluidos en este documento.

Comentario: Esta política impide a los usuarios y otras personas refutar la autoridad del departamento de Seguridad Informática para crear y modificar las normas técnicas y los procedimientos operativos. Esta política crea las bases para el desarrollo y adquisición de documentos más detallados. Cada norma o procedimiento que se pretenda convertir en una extensión de este documento de política, debe incluir las palabras, "Esta norma o procedimiento ha sido creado en concordancia con la autoridad establecida en la Política de Seguridad Informática de la Empresa X y debe ser cumplido como si fuera parte de dicho documento". La política le permite a Seguridad informática enfocarse en lo que está pendiente, en lugar de reinventar la rueda, en términos de estructuras organizacionales, responsabilidades y autorizaciones gerenciales relativas a la seguridad informática.

Políticas Relacionadas:[“Seguridad Informática Centralizada”](#) y [“Control de los Activos Informáticos”](#)

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

14. Planes de Seguridad Informática

Política: Conjuntamente con la gerencia correspondiente, el departamento de Seguridad Informática debe preparar planes anuales para el mejoramiento de la seguridad de todos los sistemas informáticos de la Empresa X.

Comentario: Esta política exige que el personal del departamento de Seguridad Informática y los gerentes de otros departamentos preparen anualmente un plan formal para mejorar la seguridad informática. Gran parte del trabajo en el campo de la seguridad informática es manejar problemas urgentes, y el personal de Seguridad Informática debe periódicamente revisar lo que se hace ahora y lo que debe hacerse. En otras palabras, esta política requiere personal enfocado en lo que es importante, no sólo en lo que es urgente. Esta política informa que esta revisión no sólo debe hacerla el personal de Seguridad Informática, sino también la gerencia de otros departamentos importantes. Esta política indirectamente apoya la evaluación periódica de riesgos. Sin el conocimiento específico de los riesgos y vulnerabilidades actuales, una organización no puede preparar planes de seguridad informática que realmente respondan a sus necesidades empresariales. El término "planes" puede cambiarse por "plan" si es necesario. Se utilizó el plural en esta política debido a que el trabajo a realizar probablemente aparecerá en diversos lugares, tales como en los presupuestos de los departamentos usuarios, el presupuesto central de Seguridad Informática o el presupuesto de Recursos Humanos.

Políticas Relacionadas: “Clasificación del Software y los Sistemas,” “Planes de Recuperación Ante Desastre Computacional,” “Planes de Respuesta Ante Emergencias Computacionales,” “Planes Divisionales para el Cumplimiento de la Seguridad Informática,” “Análisis de Violaciones y Problemas,” y “Seguridad Informática Centralizada”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

15. Manual de Seguridad Informática

Política: El departamento de Seguridad Informática debe preparar, mantener y distribuir uno o más manuales de seguridad informática que describan con exactitud las políticas, las normas y los procedimientos de seguridad informática de la Empresa X.

Comentario: Esta política exige a Seguridad Informática preparar y mantener un documento que describa los procedimientos de la Empresa X. Sin instrucciones en seguridad informática, es difícil justificar medidas disciplinarias contra los empleados. Sin instrucciones escritas, puede ser problemático ejercer la autoridad para sensibilizar a las personas acerca de la necesidad de la seguridad informática y el esfuerzo que conlleva el adiestramiento respectivo. El manual debe incluir cómo manejar correos internos de distintos cortes, contraseñas, identificadores de usuario y demás tópicos orientados al usuario. El contenido del manual no debe mencionarse puesto que su contenido varía cada año. Esta política requiere que las filiales, divisiones u otras unidades organizacionales准备 sus propios manuales y la responsabilidad por los mismos puede asignarse al departamento de adiestramiento. Si no se indica cuál organización es responsable, seguro habrá confusión. La necesidad de esta política proviene del hecho de que la seguridad informática es multidisciplinaria, multidepartamental y cada vez más multiorganizacional. La palabra "instrucciones" podría utilizarse en lugar de "manuales" y la palabra "manuales" no quiere decir un documento en papel, porque puede residir en la intranet de la empresa, en un servidor de red de área local, en un foro electrónico o estar disponible a través de cualquier otro medio electrónico.

Políticas Relacionadas: “Documentación de Adiestramiento y Operaciones,” “Adiestramiento en Seguridad Informática,” y “Tiempo de Adiestramiento”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

16. Enlaces de Seguridad Informática

Política: Cada gerente de departamento debe designar un enlace de seguridad informática y suministrarle suficiente adiestramiento, materiales de apoyo y otros recursos para realizar adecuadamente su trabajo.

Comentario: Esta política informa a los gerentes departamentales y a las gerencias de niveles bajos que los enlaces de seguridad informática son importantes y deben ser apoyados adecuadamente. Como seguridad informática no genera ganancias directas, la gerencia puede asumir erróneamente que no es importante. La política es conveniente para aquellas organizaciones que tienen enlaces a medio tiempo. Los enlaces a menudo actúan como contactos locales en materia de seguridad informática y como conocedores de la misma, ya que se desempeñan frecuentemente como administradores de

una red de área local o de la seguridad encargados del control de acceso a los sistemas. Esta política es importante para los departamentos que utilizan computadores personales y estaciones de trabajo, redes de área local o sistemas cliente-servidor.

Políticas Relacionadas:“[Administrador de Seguridad Designado](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

17. Asignación de la Propiedad de la Información

Política: La gerencia ejecutiva debe asignar la responsabilidad de la propiedad a un único individuo interno que haga el mayor uso de la información.

Comentario:Esta política aclara cómo deben ser designados los Propietarios de la información. Si los criterios no son específicos, a menudo no se designará el Propietario y, como consecuencia, la seguridad de la información correspondiente será deficiente. Con intranets, las bases de datos integradas distribuidas, los sistemas de cliente-servidor y otras aplicaciones multidepartamentales, la asignación de la propiedad puede ser un asunto importante. El término "mayor uso" es ambiguo debido a que cada decisión dependerá de factores diferentes, muchos de los cuales estarán enlazados a actividades empresariales estratégicamente importantes. Otra forma de determinar la propiedad es identificar quién paga la factura por el almacenamiento y los otros servicios informáticos asociados con la información. La propiedad puede ser determinada mediante la identificación del gerente responsable por mantener la información o los sistemas informáticos correspondientes.

Políticas Relacionadas:“[Propiedad de la Información](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

18. Responsabilidad de la Propiedad en el Departamento de Sistemas Informáticos

Política: Con excepción de la información operacional relativa a los computadores y a la red, el departamento de Sistemas Informáticos no debe ser Propietario de ninguna información.

Comentario:Esta política aclara que el departamento de Sistemas Informáticos, que a menudo funge de Custodio, no debe ser también el Propietario de la información. Esto crea un conflicto de intereses donde la seguridad probablemente resultará perjudicada. Por ejemplo, Sistemas Informáticos puede decidir utilizar controles mínimos para la información confidencial, ya que esto acelera el acceso y mantiene bajos los costos. El término "Sistemas Informáticos" puede ser remplazado por "Tecnología Informática" u otros términos utilizados en la organización.

Políticas Relacionadas:“[Propiedad de la Información](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

19. Propiedad Predeterminada de la Información

Política: Si la propiedad de un tipo específico de información residente en un computador multiusuario de producción no ha sido claramente asignada a un gerente específico, recaerá temporalmente en el gerente de Operaciones Computarizadas.

Comentario:Esta política señala al Propietario de la información de producción hasta que un Propietario oficial sea designado por la alta gerencia. Mientras tanto, el gerente de Operaciones Computarizadas tiene el rol de Custodio y toma decisiones, como Propietario, sobre la misma información. Hay necesidad de un Propietario temporal en muchos casos, ya que el gerente que supuestamente actúa como Propietario de la información puede que ni siquiera sepa cuáles son sus obligaciones, ni esté realizándolas, o quizás ni ha aceptado hacerse cargo de esas obligaciones o tal vez se encuentra discutiendo la designación de la propiedad en ese momento. Entretanto, los datos de producción deben estar protegidos adecuadamente, actualizados y manejados de tal manera que el trabajo diario se complete. Es razonable que el gerente Operacional de Computación haga las veces del Propietario, al menos por un corto período de tiempo.

Políticas Relacionadas:“[Responsabilidad de la Propiedad en el Departamento de Sistemas Informáticos](#)” y “[Custodio de la Información](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

20. Custodio de la Información

Política: Cada tipo importante de información debe tener un Custodio designado, quien ha de proteger apropiadamente la información de la Empresa X, en tanto cumpla las instrucciones emitidas por el Propietario designado en lo relativo al control de acceso, la confidencialidad y la criticidad de los datos.

Comentario: Esta política requiere la designación de un Custodio para cada tipo significativo de información. Para determinar si la información es significativa, la organización puede investigar si la información está incluida en un diccionario de datos que abarque toda la organización. Otro objetivo de la política es asignar las responsabilidades de los Custodios de la información. Esta política también implica que los Propietarios deben pagar a los Custodios por proteger adecuadamente la información correspondiente. Esto puede manifestarse a través de un sistema interno de reversión de cargos, de los precios de transferencia inter-organizacional o cualquier otro mecanismo de contabilidad. Si el Propietario no proporciona suficientes recursos para proteger la información, el Custodio debe entonces notificar al Propietario que la información no está protegida en concordancia con las instrucciones emitidas. Aun cuando los Custodios pueden ser individuos u organizaciones, es mejor si se limita el cargo a personas, ya que esto promueve la responsabilidad que se busca. Algunas organizaciones querrán aumentar las responsabilidades ya establecidas para incluir el suministro y el mantenimiento de un sistema general de seguridad para sistemas informáticos.

Políticas Relacionadas: “Control de los Activos Informáticos,” “Partida Presupuestaria para la Seguridad Informática,” y “Inventario de Activos — Información”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

21. Responsabilidades del Custodio de la Información

Política: Los Custodios de la información son responsables de definir procedimientos de control específicos, administrar el control de acceso a la información, implementar y mantener medidas de bajo costo del control de acceso a la información, y suministrar capacidades de recuperación, en concordancia con las instrucciones de los Propietarios de la información.

Comentario: Esta política define lo que significa ser un Custodio de la información. Por ejemplo, la política especifica que los Custodios no toman todas las

decisiones de seguridad relativas a la información. Los Custodios, en cambio, proporcionan un servicio adaptado a las instrucciones de los Propietarios. Esta política está redactada de forma tal que asume que, desde el punto de vista organizacional, Seguridad Informática reporta a Sistemas Informáticos. Si no es así, será necesario eliminar de esta política la referencia a la administración de controles de acceso. Lo ideal sería que las responsabilidades fuesen asignadas de tal manera que Seguridad Informática no se convierta en Custodio de ninguna información de producción.

Políticas Relacionadas: “Custodio de la Información”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

22. Responsabilidades del Usuario de la Información

Política: Todos los usuarios de la información de la Empresa X deben cumplir los requisitos de control especificados por el Propietario o Custodio de la información.

Comentario: Esta política notifica a los usuarios que pueden utilizar la información siempre y cuando la protejan adecuadamente. Algunas organizaciones hacen esta política más específica al requerir que los usuarios firmen una declaración en la cual aceptan regirse por las políticas y procedimientos de Seguridad Informática. La firma en un formulario que contenga esta declaración y quizás un resumen con las políticas y procedimientos, puede ser lo que se solicite del usuario antes de entregarle su identificador de usuario y contraseña. Debe enfatizarse a los usuarios que no controlan ni son Propietarios de la información a la que se les ha permitido acceso, y no deben tomar decisiones relacionadas con la seguridad de dicha información. Sin una declaración escrita a estos efectos, los usuarios podrían decidir compartir la información con cualquiera que lo solicite. Mientras más y más información es distribuida en la intranet, redes de área local, computadores personales y sistemas de cliente-servidor, hay más necesidad urgente de políticas como ésta para aclarar las responsabilidades de seguridad de los usuarios.

Políticas Relacionadas: “Propiedad de la Información” y “Resolución de Problemas de Seguridad Informática”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

23. Delegación de la Propiedad de la Información

Política: La responsabilidad de especificar controles de información apropiados por parte del Propietario de la información no debe ser delegada a proveedores de servicios fuera de la Empresa X.

Comentario: Esta política asegura que quienes estén dentro de la empresa, que generalmente tienen un mejor entendimiento del negocio y sus necesidades que aquéllos fuera de la empresa, tomen las decisiones sobre la seguridad informática. Aquéllos fuera de la empresa pueden estar comprometidos a maximizar las ganancias y minimizar el tiempo en que su propio personal se involucra con el cliente, dando como resultado un desgaste significativo en la seguridad. La gerencia de la organización debe tomar las decisiones fundamentales sobre seguridad. La implantación actual de las decisiones sobre seguridad puede ser completada por personas externas. Esta política puede ser incorporada dentro de los acuerdos hechos fuera de la empresa, acuerdos con la gerencia de instalaciones o solicitudes a consultores de propuestas.

Políticas Relacionadas: “Propiedad de la Información” y “Resolución de Problemas de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

24. Políticas de Acceso a la Información

Política: Las políticas de acceso a la información deben ser desarrolladas de manera que especifiquen que los Propietarios de información designados, son responsa-

bles de establecer y poner al día políticas escritas pertinentes a las categorías de personas a quienes les será permitido acceder a la información por la cual serán responsables.

Comentario: Esta política notifica a los Propietarios de la información que deben tomarse el tiempo para especificar quien podrá y quien no podrá acceder a la información para la cual han sido designados como Propietarios. La razón de estas decisiones será expresada en una política de derecho al acceso. Una especificación de estos derechos de acceso es una medida necesaria para la implantación de un paquete de control de acceso basado en contraseña o las facilidades originales para un control de acceso encontradas en muchos sistemas operativos. Si se intenta implementar un paquete de control de acceso sin haber decidido cuáles van a ser las reglas, puede resultar en confusión. Esta política informa a la gerencia y al personal técnico que tales políticas sobre acceso a la información deben, no sólo ser especificadas sino que deben estar por escrito. Si estas políticas están escritas, entonces también serán auditables. Esta política es efectivamente una política de alto nivel que establece el escenario para políticas de control de acceso más específicas. A diferencia de otras políticas de seguridad informática, sólo la estructura general es pautada por la gerencia de Seguridad Informática, mientras las políticas específicas de control de acceso provienen de otras gerencias designadas.

Políticas Relacionadas: “Propiedad de la Información” y “Otorgamiento de Privilegios del Sistema”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4.01.04 Proceso de Autorización para el Procesamiento de la Información

1. Control de Nuevas Tecnologías

Política: En cada instancia donde se utilice nueva tecnología en un sistema informático de producción en la Empresa X, las operaciones y controles de seguridad asociados a la nueva tecnología deben ser particularmente rigurosos hasta que se demuestre que la nueva tecnología es confiable, rápidamente controlable y que es un verdadero apoyo a las actividades del negocio.

Comentario: Esta política conservadora refleja una sabia práctica cuando se trata de nueva tecnología. Básicamente dice que hasta que la nueva tecnología se haya comprobado se necesitan controles extras. Pero,

aún después que la nueva tecnología se haya comprobado, la eliminación o liberación de los controles relacionados deben requerir autorización por la gerencia de Seguridad Informativa. Esta política refleja que es mucho más fácil liberar los controles que ajustarlos. Los usuarios recibirán gratamente lo primero pero se quejarán amargamente de lo último. Los trabajadores usualmente acatan estos controles adicionales puesto que lo ven como la manera de obtener la capacidad que proporciona la nueva tecnología.

Políticas Relacionadas: “Inhabilitación de Componentes Críticos de Seguridad” e “Identificación de Requisitos de Seguridad”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

2. Inhabilitación de Componentes Críticos de Seguridad

Política: Los componentes críticos de la infraestructura de seguridad informática de la Empresa X, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la gerencia de Seguridad Informática.

Comentario:Esta política está motivada por la tendencia natural de los administradores de sistemas a responder rápidamente a las quejas de los usuarios. La política informa a los administradores y otros trabajadores que no pueden remover un control crítico sin

obtener la autorización necesaria. Esta política adopta el balance adecuado entre la seguridad informativa y otros objetivos del negocio. En esta instancia el objetivo que les compete se está logrando. La política, deliberadamente evita una definición para un componente crítico, estimulando por lo tanto en el lector de esta política la inquietud de buscar una directriz e interpretación gerencial. Una definición específica de un componente crítico tampoco es recomendable debido a que este conjunto de controles cambiará significativamente con el correr del tiempo.

Políticas Relacionadas:“[Software Innecesario](#)” e “[Intentos de Introducir Contraseña](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

4.01.05 Consejo Especializado en Seguridad Informática

1. Evaluación del Riesgo en los Sistemas de Producción

Política: Todos los sistemas computarizados de producción deben ser evaluados periódicamente por la gerencia de Seguridad Informática para determinar el mínimo conjunto de controles requeridos para reducir y mantener el riesgo a un nivel aceptable.

Comentario:El proceso descrito en la política es una evaluación de riesgo, llamado también análisis de riesgo. La política requiere una evaluación del riesgo que corren todos los sistemas informáticos de producción para asegurarse que los sistemas críticos del negocio han recibido al menos un nivel rudimentario de atención en seguridad. Algunos lectores pueden desear colocar un período de tiempo dentro de la política, aunque simplemente usar el término "periódico" es recomendado. De la forma en que la política está escrita ahora, los sistemas de producción pueden ser priorizados por riesgo, y aquéllos que presenten un riesgo mayor pueden ser examinados frecuentemente y

en detalle. Estas evaluaciones pueden ser llevadas a cabo por Auditoría Interna o Auditoría de Tecnología informática en lugar del departamento de Seguridad Informática. Es recomendable especificar cuál grupo es responsable de la evaluación de riesgo bien sea a través de esta política o una política separada que se ocupe de todas las responsabilidades. Una evaluación de riesgo proporciona información de fondo en la cual la gerencia de seguridad informática se basa para tomar decisiones con respecto a presupuestos, planes sobre personal y planes de proyectos.

Políticas Relacionadas:“[Riesgos Significativos para la Seguridad Informática](#),” “[Tareas del Departamento de Seguridad Informática](#),” “[Planes de Seguridad Informática](#),” y “[Controles Mínimos en Sistemas Informáticos](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

4.01.06 Cooperación Entre Organizaciones

1. Divulgación de Productos de Seguridad Informática

Política: No deben divulgarse en ningún momento el nombre de los productos, los proveedores involucrados y las configuraciones asociadas con los sistemas de

seguridad informática instalados en la Empresa X, a menos que se obtenga el permiso previo de la gerencia de Seguridad Informática.

Comentario: Esta política impide al personal mencionar a terceros la tecnología utilizada para proteger la información de la Empresa X. El personal puede pensar que dicha divulgación es algo por lo cual no tienen que preocuparse, pero en realidad esta información puede ser vital para comprometer los sistemas de la Empresa X. Esta política niega control de la información a aquéllos que no tienen necesidad de ella. Esto no significa seguridad por encubrimiento, sino el resguardo de la información que puede ser útil al adversario. Como efecto secundario, esta política también impide a los trabajadores patrocinar cualquier información sobre productos de seguridad.

Políticas Relacionadas: “Notas de Prensa Sobre Información de Vulnerabilidad” y “Comunicaciones Públicas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

2. Divulgación Pública de Información Empresarial

Política: La Empresa X no debe divulgar públicamente ninguna información relacionada a acuerdos o transacciones empresariales de la que pueda razonablemente desprenderse un daño material para un cliente o un tercero.

4.01.07 Revisión Independiente de la Seguridad Informática

1. Uso de Investigadores

Política: La utilización de investigadores haciéndose pasar por otra persona para poner a prueba el servicio al cliente y las políticas de seguridad o investigar supuestas fechorías, debe ser autorizada por el gerente superior responsable de la seguridad física.

Comentario: Esta política notifica a los empleados que puede haber espías dentro de la organización haciéndose pasar por empleados regulares u otro personal autorizado, pero que en realidad son investigadores. Estos investigadores pueden emplear técnicas como llamadas telefónicas falsas como si fueran otras personas con el fin de obtener cierta información o para determinar las respuestas de un trabajador a ciertas preguntas. Tener una política como ésta muestra la intención de la gerencia de ir más allá y ser francos

Comentario: Esta política mantiene buenas relaciones de trabajo con clientes, socios de negocios y otros. En muchas organizaciones, el departamento de Mercadeo rápidamente anuncia al público un importante acuerdo de negocios o una transacción importante sin considerar el daño que tal anuncio puede crear. La política es deliberadamente ambigua con las palabras “daño material”. La gerencia tendrá que considerar qué constituye un daño material considerable caso por caso. Esta política es una versión empresarial de lo que los militares llaman análisis de tráfico. En otras palabras, si el enemigo descubre quién está mandando mensajes a quién, o quién está haciendo negocios con quién, es mucha la información que se puede recoger, aun cuando el contenido de los mensajes o la naturaleza del trato se desconozcan.

Políticas Relacionadas: “Notas de Prensa Sobre Información de Vulnerabilidad” y “Representaciones en Internet Que Incluyan Afiliación”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

acerca de un tema controversial, y previene alegatos futuros de haberse dejado engañar. Esta política estimula a los empleados a mostrar su mejor comportamiento. También es considerada una restricción a los derechos de privacidad porque los trabajadores no saben con quién están tratando por teléfono, por el sistema de correo o cualquier otro medio de comunicación. Tomar esta incertidumbre con seriedad es la misma actitud que muchas organizaciones buscan promover para impedir ingeniería social, burlas o engaños que conlleven serias pérdidas.

Políticas Relacionadas: “Información de Contacto del Remitente” y “Validación de la Identidad de Terceros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

2. Revisión de los Controles de los Sistemas Informáticos — Independiente

Política: Periódicamente debe llevarse a cabo una revisión externa e independiente de los controles de los sistemas informáticos para determinar su calidad y cumplimiento.

Comentario: Esta política requiere por parte de la gerencia que periódicamente busque retroalimentación externa sobre controles de los sistemas informáticos. Muchas organizaciones asumen que son seguras cuando en realidad no se han dado cuenta de las vulnerabilidades que enfrentan. Este problema es particularmente serio en organizaciones en las que la gerencia de Sistemas Informáticos ha estado empleada por esa misma organización durante muchos años. En estos casos, el personal se torna complaciente y no se mantiene al día ni con la tecnología ni con los riesgos que presenta. Una revisión hecha por un agente externo es una manera útil de superar las lealtades internas y los conflictos de interés que han conspirado para mantener esas vulnerabilidades ocultas. También es útil que un

tercero independiente suministre un chequeo de la realidad, particularmente para garantizar que se están utilizando las normas de debido cuidado. Durante la auditoría financiera se requieren auditores externos para observar los controles computacionales internos. Ellos examinan los controles para determinar hasta dónde pueden confiar en los resultados de los sistemas que utilizan estos controles. Sin embargo, en una auditoría financiera, los auditores externos no investigan los controles de sistemas informáticos en profundidad para detectar otras vulnerabilidades no directamente asociadas con sistemas informáticos financieros. Es por ello que la revisión adicional suministrada por un consultor técnico externo o un especialista es lo más apropiado.

Políticas Relacionadas: “[Controles Mínimos en Sistemas Informáticos](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4.02 Seguridad en el Acceso de Terceros

4.02.01 Identificación de Riesgos Originados por Acceso de Terceros

1. Identificadores de Usuario para Terceros

Política: No debe otorgarse identificador de usuario ni privilegios para utilizar los computadores o los sistemas de comunicación de la Empresa X a las personas que no sean empleados, a contratistas o consultores, a menos que se obtenga la autorización escrita del gerente del departamento.

Comentario: La intención de esta política es garantizar que terceros no autorizados no utilicen los recursos de la Empresa X sin el conocimiento y autorización específica de la gerencia. Esta política también garantiza que los clientes o proveedores de servicios se mantengan fuera de los sistemas de la Empresa X, a menos que el gerente así lo autorice. La autorización puede ser otorgada por el gerente de Seguridad Informática u otro gerente con responsabilidad sobre los sistemas de toda la organización. Algunas organizaciones utilizan una variación de esta política que consiste en el respaldo que un gerente debe darle a un tercero antes de emitirle un identificador de usuario. La palabra "temporal" no aparece con los términos "empleados, contratistas o

consultores", ya que los temporales normalmente son contratados con muy poca verificación de sus antecedentes.

Políticas Relacionadas: “[Acceso a la Red](#),” “[Identificador Único de Usuario y Contraseña Obligatorios](#),” “[Formularios para Identificadores de Usuario](#),” y “[Reautorización de los Privilegios de Acceso de Usuario](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Privilegios de Trabajadores Temporales

Política: Los trabajadores temporales no deben recibir privilegios sobre los sistemas informáticos de la Empresa X, a menos que el Propietario de la información lo autorice por escrito.

Comentario: Esta política limita los privilegios sobre los sistemas informáticos a aquellos que han sido objeto de revisiones de antecedentes y que a través del tiempo han demostrado ser confiables. Normalmente, los empleados temporales no cuadran en estas categorías y

generalmente trabajan con una organización específica a lo sumo un par de meses y la gerencia tiene poco incentivo para invertir en ellos, incluyendo la revisión de los antecedentes y el suministro de adiestramiento. Desde otro punto de vista, los empleados temporales tienen muy poca lealtad hacia un jefe específico. Recientemente la preocupación sobre el espionaje y terrorismo industrial se ha incrementado, lo que ha llevado a muchas organizaciones a considerar a los empleados temporales como no confiables. Esta política asume que las responsabilidades de los Propietarios de la información han sido definidas en otra política.

Políticas Relacionadas: "Identificadores de Usuario para Terceros," "Revisión de Antecedentes de No Empleados," y "Acceso para Trabajadores Temporales y Consultores"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

3. Acceso Remoto de Terceros

Política: No debe concederse a proveedores externos la entrada a la red o a Internet vía telefónica, ni privilegios a las redes privadas virtuales, a menos que tengan una necesidad legítima de negocio para tal acceso y siempre que sean permitidos a personas específicas y sólo por el tiempo requerido para cumplir las tareas autorizadas.

Comentario: La conexión a la red o Internet por discado y los privilegios a las redes privadas virtuales han sido utilizados por un número de atacantes para obtener acceso no autorizado a los sistemas. No es recomendable dejar estos puertos abiertos y disponibles, como aquéllos utilizados por los proveedores para mantenimiento remoto, si no se están utilizando. Esta política conserva los puertos de mantenimiento apagados y excluye así a terceros del sistema a menos que hayan obtenido la autorización de la gerencia de la Empresa X. Tener un proceso formal de autorización también desmotiva, si no evita, que otros intenten hacerse pasar por representantes de proveedores. Para reducir la cobertura de esta política se cambia la palabra "privilegios" por "privilegios de mantenimiento". Esta política puede expandirse para aplicarse a intercambios privados entre sucursales, cambios de puntos de conexión de redes y otros sistemas de comunicación y sistemas generales de computación como minicomputadores y mainframes. El uso de la palabra "entrada" proporciona una excepción para los sofisticados sistemas de mantenimiento que automáticamente discan el número del sistema del vendedor al detectar un problema.

Políticas Relacionadas: "Activación del Puente de Conferencias" y "Conexiones Discadas"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Anotaciones de los Consultores

Política: Los consultores de la Empresa X no deben tomar notas acerca de las reuniones confidenciales con sus clientes.

Comentario: Esta política garantiza a los clientes que la información escrita sobre sus asuntos privados no caerá en manos de terceros no autorizados. La política es adaptada de una declaración emitida por un psicólogo, donde refleja la inquietud de que se revele información de sus pacientes a través de una demanda legal o de un robo. El psicólogo confía en su memoria para servir a sus pacientes y, por lo tanto, no se preocupa si sus archivos confidenciales son examinados por terceros. Esta política se puede adaptar fácilmente a otras líneas de trabajo. Esta política asume que el trabajo puede ser realizado sin tomar notas. En otros trabajos esto es sencillamente imposible de realizar porque las tareas son demasiado complejas para ser eficientes sin tomar notas de algún tipo como en el área de sistemas informáticos.

Políticas Relacionadas: “Divulgación de la Información del Cliente” y “Enlaces con Información Privada”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

5. Acuerdo de Confidencialidad para el Personal de Reparación de Máquinas de Oficina

Política: Todo el personal externo de reparación de equipos de oficina debe firmar un acuerdo de confidencialidad con la Empresa X antes de comenzar su trabajo.

Comentario: Esta política evita el espionaje industrial o militar. Los modelos recientes de equipos de oficinas, como copiadoras y máquinas de fax, tienen hasta cinco megabites de información reciente almacenada en ellas. Si un trabajador de reparación intercambia un chip que contenga esta información se adueña de propiedad intelectual sin ser detectado. Si se atasca el papel, puede haber información confidencial en el papel atascado. La política está redactada con un enfoque amplio para incluir en este rango los computadores de uso general y los personales. Algunas organizaciones se refieren a los acuerdos de confidencialidad como acuerdos de no divulgación.

Políticas Relacionadas: “Acuerdos de Confidencialidad,” “Términos y Condiciones para el Acceso de Terceros,” y “Medios de Almacenamiento de Información Sensible”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

6. Diseminación de la Información

Política: El acceso de terceros a cualquier información interna de la Empresa X se concede sólo demostrando la necesidad de conocerla y cuando tal divulgación esté expresamente autorizada por la gerencia de la Empresa X.

Comentario: Esta política informa a los trabajadores que, en ausencia de instrucciones adicionales, debe limitarse la diseminación de la información interna de la Empresa X. Esta es una buena política general en la cual pueden apoyarse otras declaraciones más explícitas o puede ser suficiente para aquellas organizaciones que no poseen mucha información confidencial. Esta política se aplica en aquellas organizaciones que aún no poseen un sistema formal de clasificación de datos. En esta política no se hace mención de etiquetas de clasificación de datos; sin embargo, las etiquetas pueden ahorrar tiempo y dinero además de normalizar el manejo de información sensible. Esta política es importante para las organizaciones con conexiones a Internet u otras redes de computadores públicos. Casos recientes señalan que los empleados distribuyen información interna en foros electrónicos, en sesiones de chat en Internet y en otros foros públicos, a menos que específicamente no se permita. Restringir el flujo de información interna hacia redes externas también es posible con ciertos controles de cortafuegos, como aquellos que examinan el contenido de los datos enviados. La política no utiliza acuerdos formales de confidencialidad.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Mal Funcionamiento del Control de Acceso”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7. Acuerdos de Confidencialidad — Terceros

Política: Antes de enviarse cualquier información secreta, confidencial o privada a un tercero para copiar, imprimir, formatear u otro tipo de manejo, dicho tercero debe firmar un acuerdo de confidencialidad con la Empresa X.

Comentario: Esta política define claramente el límite para el movimiento de información confidencial. Si se asume que todos los trabajadores de la Empresa X han firmado acuerdos de confidencialidad, los tipos de información a que se hace referencia pueden circular dentro de la organización sin controles adicionales. Pero los terceros fuera de la organización, por lo general, no han firmado estos acuerdos que se requieren antes de entregarles la información confidencial interna. Un ejemplo sería la imprenta que prepara el reporte público anual de una compañía. Esta imprenta debe firmar un acuerdo de confidencialidad para evitar que sus trabajadores internos hagan uso indebido de la información contenida en el reporte para realizar transacciones ilegales. Esta política es importante para medios de almacenamiento de datos en correos electrónicos, computadores y papel común y corriente. Como resultado, la política no menciona específicamente la tecnología que puede ser empleada, pero puede incluir comentarios que la expliquen. La política que se señala puede ser redactada de manera que las palabras "secreta, confidencial o privada" sean remplazadas con las etiquetas específicas de clasificación de datos utilizadas dentro de la organización.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Acuerdos de Confidencialidad — Organización](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Acuerdos de Confidencialidad

Política: Toda divulgación de información secreta, confidencial o privada de la Empresa X a terceros se hará a través de la firma de un acuerdo de confidencialidad que incluya restricciones a la subsiguiente diseminación y manejo de la información.

Comentario: Esta política evita el uso no autorizado de la información de la Empresa X, incluyendo la diseminación secundaria. Instrucciones específicas sobre el uso deberían prohibir la distribución adicional sin el consentimiento del Propietario. Esta política puede expandirse para delinejar los requerimientos específicos

que deben ser declarados como parte de un acuerdo de confidencialidad, los cuales pueden incluir la devolución de la información, cómo será utilizada, para qué va a ser utilizada y quién recibirá acceso a la misma.

Políticas Relacionadas: “[Diseminación Secundaria de la Información Secreta](#),” “[Manejo de Información Sensible](#),” y “[Convenio de Cumplimiento](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9. Acceso para Trabajadores Temporales y Consultores

Política: Las actividades que requieren acceso a información sensible de la Empresa X deben ser realizadas únicamente por empleados permanentes a tiempo completo, a menos que no posean el conocimiento o las habilidades necesarias, o que una emergencia exija la presencia de trabajadores adicionales o se tenga la autorización del director de Recursos Humanos y la del Propietario de la información.

Comentario: Esta política limita el acceso a la información confidencial únicamente a los individuos más confiables. Generalmente, los empleados permanentes a tiempo completo son más leales que los temporales, los contratistas o los consultores y, por lo tanto, más confiables. Una vez que la relación de trabajo ha terminado, la Empresa X tiene muy poco control sobre las actividades de empleados temporales, consultores o contratistas, pero sí mantiene cierto control sobre ex-empleados de tiempo completo. Los riesgos de utilizar personas que no sean empleados permanentes a tiempo completo es parcialmente mitigada con los acuerdos de confidencialidad y convenios de no competencia. Las entidades que son corporaciones virtuales, que utilizan extenso personal externo de otras empresas o que poseen otras estructuras organizacionales descentralizadas o a través de la red, pueden tener problemas con esta política pues está basada en la presunción de que un grupo esencial de empleados está al mando de la organización.

Políticas Relacionadas: “[Acuerdos de Confidencialidad — Organización](#),” “[Clasificación de Datos en Cuatro Categorías](#),” y “[Restricción de Privilegios — Necesidad de Conocer](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

10. Guías Telefónicas Internas

Política: Las guías telefónicas internas no deben ser distribuidas a terceros distintos de contratistas, consultores, trabajadores temporales y otros terceros que trabajan para la Empresa X, sin la autorización específica de un gerente departamental.

Comentario: Esta política cambia la manera de pensar acerca de la información contenida en una guía telefónica interna. Como reflejo de esto, muchas organizaciones han añadido la palabra "confidencial" o "restringida" a cada página o a la cubierta de sus guías telefónicas. Las guías telefónicas son utilizadas por reclutadores de personal para ubicar candidatos potenciales. De manera similar los espías industriales utilizan las guías telefónicas para identificar trabajadores que deseen sobornar, presionar, engañar o explotar. Los hackers también utilizan este libreto para identificar números de modem y otros números relacionados con los sistemas. Adicionalmente, los espías industriales pueden utilizar las guías telefónicas como una forma de deducir a quién simular en sus intentos de ingeniería social. Esta política puede llevarse más allá al restringir la diseminación de la información contenida en la guía. Por ejemplo, si alguien telefonea a la Empresa X solicitando el nombre y el número telefónico del director de Seguridad Informática, el operador tiene prohibido suministrar esta información. La consecuencia de designar una guía telefónica interna como confidencial es que debe ser eliminada de forma segura. Algunas empresas indican en las portadas "Toda Vez Que Se Publique Una Nueva Guía, Devuelva Esta Guía Al Departamento De Seguridad Para su Eliminación Correspondiente".

Políticas Relacionadas: ["Números de Acceso a Computadores"](#)

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

11. Acceso de Terceros a Sistemas Internos

Política: El coordinador de seguridad informática designado debe autorizar el acceso de terceros a los sistemas internos de la Empresa X distintos de aquéllos claramente públicos.

Comentario: Esta política evita que los administradores de sistemas u otros, alegremente autoricen el acceso de terceros a las máquinas y sistemas internos. La extranet se ha convertido en un sistema muy popular y, en su afán de explotarlo, los gerentes autorizan el acceso a terceros sin seguir los procesos autorizados de control

de acceso. Se indica la participación del coordinador de seguridad informática porque estos representantes de una infraestructura centralizada conocen las reglas establecidas para autorizar los privilegios del control de acceso. En la política, el coordinador de seguridad informática puede ser remplazado por la gerencia de seguridad informática u otros que formen parte de la infraestructura centralizada de seguridad informática existente. En la medida en que los sistemas informáticos se descentralizan y distribuyen, los usuarios finales asumen los roles de los administradores de los sistemas y se colocan en posición de poder autorizar el acceso a terceros. Esta política cubre varios tipos de accesos, tales como cuentas de correo electrónico, identificador de usuario de acceso a Internet y aplicaciones verificadoras de inventario.

Políticas Relacionadas: ["Restricción de Privilegios — Necesidad de Conocer"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Responsabilidades de Terceros en la Seguridad Informática

Política: Previo al contacto que los usuarios de un tercero hagan con los sistemas de la Empresa X a través de conexiones informáticas en tiempo real, se requiere autorización escrita dada por la gerencia de Seguridad Informática especificando las responsabilidades relacionadas a la seguridad de la Empresa X, las del proveedor de la conexión y las de todos los terceros involucrados.

Comentario: Esta política evita las conexiones en tiempo real del sistema de la Empresa X con terceros, a menos que se demuestre que son seguras. Esta política evitaría, por ejemplo, que los vendedores abrieran el sistema de pedidos de los clientes a menos que los controles de seguridad hayan sido examinados e implementados apropiadamente. Sólo después de haber especificado claramente las responsabilidades de seguridad puede la Empresa X determinar si desea aceptar los riesgos que presenta la conexión. La política permite a los usuarios internos emplear sistemas de llamadas salientes para acceder a los servicios de correo electrónico de terceros y los de base de datos en línea sin necesidad de efectuar una evaluación de seguridad y un proceso de autorización. Esta política permite realizar conexiones de Internet para correo electrónico puesto que no son conexiones en tiempo real. Sin embargo, esta política evitaría que un departamento establezca su propio cortafuego de Internet.

Políticas Relacionadas: “[Interconexión de Sistemas](#),” “[Cambios en la Línea de Comunicación](#),” y “[Conexiones a Internet](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

13. Condición Financiera de Proveedores Importantes

Política: El jefe principal de informática, o su delegado, debe revisar anualmente las condiciones financieras de los proveedores que suministran o respaldan los sistemas informáticos de producción críticos para la Empresa X.

Comentario: Esta política exige que aquellos responsables del manejo de los sistemas informáticos consideren periódicamente la condición financiera de los proveedores esenciales. Con las adquisiciones, fusiones, bancarrotas, ofertas públicas iniciales y otros eventos frecuentes en la industria de la informática, las relaciones con los proveedores pueden cambiar rápidamente. Una gran cantidad de productos y servicios de

sistemas informáticos son suministrados por proveedores externos y las organizaciones compradoras se hacen mucho más dependientes de dichos proveedores. Si la gerencia tiene dudas con respecto a la viabilidad financiera de un proveedor, puede tomar medidas compensatorias como, por ejemplo, adquirir una garantía ejecutable para el software, establecer contratos de apoyo con otros proveedores e investigar las formas en que puede convertir los datos de producción al software de otros proveedores. Esta política está redactada en forma general para incluir tanto servicios como productos. En sus contratos, muchas organizaciones piden a proveedores privados revelar sus declaraciones financieras anuales para cumplir así con lo exigido en esta política. Se recomiendan revisiones financieras trimestrales o incluso mensuales de los proveedores particularmente inestables o riesgosos.

Políticas Relacionadas: “[Instalación de Software de Sistemas Proporcionado por Proveedores](#)” y “[Enunciados de la Integridad del Software](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4.02.02 Requisitos de Seguridad en Contratos con Terceros

1. Términos y Condiciones para el Acceso de Terceros

Política: Antes de recibir acceso a los sistemas de la Empresa X, un gerente en representación de la organización del tercero debe firmar un contrato donde se definan los términos y condiciones del acceso, y éste debe ser autorizado por Seguridad Informática y por el vicepresidente del departamento Legal de la Empresa X.

Comentario: En muchas organizaciones se otorga el acceso a los sistemas internos, a grupos y consultores externos, a contratistas y otros terceros como si de trabajadores confiables se tratase. Esto puede ocasionar serias fallas de seguridad, especialmente si los sistemas no están protegidos adecuadamente. Esta política tiene la intención de notificar a todo el personal interno que el acceso otorgado a terceros es un asunto serio de seguridad y que, en todas las instancias, debe estar apoyado por un contrato escrito y autorizado. Luego de repetir el proceso varias veces, los gerentes internos que aprueban este tipo de contrato desarrollarán un listado de los criterios que deben ser incluidos en cada contrato. Esta lista puede ser utilizada para desarrollar un contrato para todos los terceros que deseen acceso a los sistemas informáticos internos. Este contrato normalmente

aborda cosas tales como el acuerdo de confidencialidad, la descripción de las medidas específicas de control que deben ser utilizadas para los datos de la Empresa X, cómo reaccionar en caso de darse una falla de seguridad y la asignación de la responsabilidad ante cualquier problema que surja.

Políticas Relacionadas: “[Revocación de Privilegios de Acceso](#)” y “[Reautorización de los Privilegios de Acceso de Usuario](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Transferencia de Información a Terceros

Política: La documentación, el software o cualquier tipo de información interna de la Empresa X no deben ser vendidos o de manera alguna transferidos a algún grupo ajeno a la Empresa X para propósitos no autorizados por la gerencia.

Comentario: Se conoce de casos de trabajadores que han vendido listas de correos u otro tipo de datos internos. Asimismo, se conoce de empleados de

organizaciones de software que han colocado copias de software en Internet antes de su salida al mercado. Esta política informa a los trabajadores que la información debe permanecer interna. La existencia de tal notificación es la base para acciones disciplinarias o demandas legales. En ocasiones, la transferencia de información a terceros es de buena fe, como cuando un empleado hace una copia de una documentación de seguridad para enseñarla a sus colegas en una asociación de profesionales de seguridad informática. En este caso, la divulgación de la información interna puede ayudar a dichos terceros a comprometer la seguridad de la organización. Algunos empleados se sentirán aliviados con esta política porque les permite rechazar la participación en encuestas de investigación, entrevistas telefónicas de investigación de mercadeo y otras interacciones que preferirían evitar.

Políticas Relacionadas: “[Convenios de Intercambio de Software y Datos](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

3. Uso por Parte de Terceros del Nombre de la Organización

Política: Ninguna organización de terceros puede utilizar el nombre de la Empresa X en sus materiales de propaganda o mercadeo, a menos que reciba el permiso del consejero legal corporativo.

Comentario: Esta política evita que las actividades de terceros desestimen el nombre de una organización. Por ejemplo, si un empresario señala que una compañía grande y prestigiosa respalda sus actividades, obtendría mayor credibilidad. Pero si lo dicho es falso y la persona termina defraudando a sus clientes, el nombre de la compañía se desestima aún cuando no haya habido falta consciente de su parte. En el peor de los casos, algunas personas podrían responsabilizar a dicha compañía por sus pérdidas, aduciendo que existió respaldo implícito. Para evitar este tipo de problemas, esta política sostiene que no es permitido el uso del nombre a menos que lo haya aprobado el consejero legal corporativo. Algunas compañías están implementando esta política de protección de marcas registradas explorando en Internet a través de motores de búsqueda, para detectar todos los sitios donde aparece su nombre. Si localizan un sitio no autorizado, contactan a los responsables y se les ordena cesar la práctica.

Políticas Relacionadas: “[Propiedad Intelectual](#)” y “[Páginas Web No Oficiales](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

4. Manejo de la Información al Finalizar el Contrato

Política: Si la Empresa X finaliza su contrato con un tercero que maneja información privada de la Empresa X, dicho tercero debe destruir o devolver inmediatamente todos los datos privados de la Empresa X que estén en su posesión.

Comentario: El propósito de esta política es especificar las formas en que se manejarán los datos privados cuando finalice la relación con un tercero que tiene custodia de datos privados. Por ejemplo, un hospital puede entregar información médica a un tercero que se encarga de cobranzas para que genere las facturas y las envíe a los pacientes. Al destruir o devolver la información se previene el uso no autorizado. Este requisito debe ser incluido en los acuerdos de confidencialidad con terceros y en los contratos de consultoría con terceros, porque un tercero no está obligado legalmente por una política interna. En este sentido, la política interna le recuerda a la gerencia y al personal técnico incluir este requisito en todos los acuerdos con terceros que manejen información privada.

Políticas Relacionadas: “[Compromiso en Acuerdos de Confidencialidad](#)” y “[Certificado de Destrucción de Medios de Almacenamiento](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Medianos y altos

5. Prohibición de Invasión de Privacidad a Través de Terceros

Política: Si la Empresa X no puede realizar cierto acto o tomar determinado curso de acción en virtud de una política de privacidad que lo impide, la Empresa X no debe contratar a uno o más terceros para que realicen dicha acción.

Comentario: A diferencia de la mayoría de las políticas de seguridad informática, la intención de esta política es que el público la conozca. Esta política garantiza a sus clientes actuales y potenciales que la Empresa X no utilizará un tecnicismo legal en su política de privacidad para evadir los requisitos de dicha política. Esta política es motivada en parte por ciertas agencias gubernamentales que han adquirido datos del sector privado a través de agentes conocidos como agregadores, los cuales se

encargan de unificar información obtenida de muchas y diversas fuentes, tales como los registros de conductores de vehículos automotores, garantías y títulos de bienes raíces, listados de números telefónicos y de registros de votantes. Estas agencias gubernamentales utilizan estos agregadores para realizar investigaciones legales y recopilar información de vigilancia que, de otra forma, estaría vedada a las agencias. Esta política garantiza a los clientes actuales y futuros que las palabras incluidas en la política de privacidad tienen significado, y que la empresa no va a recurrir a una organización externa para poder decir luego "nosotros no hicimos eso".

Políticas Relacionadas: "Medidas de Seguridad en Organizaciones de Terceros" y "Transferencia de la Información sobre Clientes"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Compromiso en Acuerdos de Confidencialidad

Política: La información privada o confidencial bajo la custodia de la Empresa X no debe ser divulgada a terceros a menos que estos terceros firmen un acuerdo explícito de compromiso con la confidencialidad aprobado por la gerencia de Seguridad Informática.

Comentario: Esta política garantiza que la información privada o confidencial no es divulgada a ningún tercero, a menos que este tercero convenga en proteger la información de la manera prescrita. El compromiso con la confidencialidad establece que el receptor de la información la devolverá cuando el proyecto termine, destruirá todas las copias de la información y se abstendrá de utilizarla para algún propósito distinto del establecido en el convenio. Otras estipulaciones pueden incluirse; por ejemplo, se puede exigir al que recibe la información que mantenga la naturaleza y existencia de la información confidencial. Un acuerdo de compromiso de la confidencialidad se puede incorporar a contratos normalizados, tales como un contrato de servicios de consultoría, o puede ser un convenio independiente. Con estos acuerdos de compromiso con la confidencialidad las empresas pueden utilizar organizaciones externas y otros negocios afiliados, con la garantía de que las políticas de seguridad informática implementadas internamente también se implementan en la organización que las recibe. Los acuerdos de compromiso con la confidencialidad son una manera rápida de sobrepasar las inconsistencias e incompatibilidades de las políticas de seguridad informática de las organizaciones. Por estas razones son populares en las extranets

y otros sistemas intranets de socios comerciales. Los acuerdos de compromiso con la confidencialidad obligan legalmente e identifican claramente al responsable de cada actividad de seguridad informática, la cual es un área importante pero a menudo olvidada.

Políticas Relacionadas: "Formularios para Identificadores de Usuario" y "Diseminación Secundaria de la Información Secreta"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7. Divulgación de las Relaciones con Proveedores

Política: Al colocar pedidos de productos o servicios, o al establecer una relación de negocios nueva o modificada, el personal de la Empresa X debe informar a los proveedores que no deben hacer pública la naturaleza ni la existencia de su relación con la Empresa X, sin la autorización escrita de un gerente corporativo de la Empresa X.

Comentario: Esta política garantiza que los proveedores no revelarán información que pueda dañar a la Empresa X o sus intereses. Los proveedores querrían publicitar sus nuevos negocios para así captar más, pero esto daña a la Empresa X ya que indirectamente revela sus estrategias, sus planes a largo plazo, la distribución de sus recursos o sus actividades actuales. Esta política evita que el nombre de la Empresa X se utilice en formas no autorizadas ni planificadas y de esta manera impide alegatos de apoyo implícito a determinado producto o servicio. Una política como ésta puede incluirse en los contratos con los proveedores. También es apropiado indicar al personal interno que deben recordar verbalmente a los proveedores sobre la existencia de esta provisión contractual.

Políticas Relacionadas: "Divulgación Pública de Información Empresarial" y "Representaciones en Internet Que Incluyan Afiliación"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

8. Recopilación de Información de Precios por Terceros

Política: Para evitar que los competidores obtengan información de propiedad interna, los terceros no deben reunir una cantidad significativa de precios de los productos o servicios de la Empresa X.

Comentario: Esta política deliberadamente pone freno al libre flujo de información. Por ejemplo, agentes de software que trabajan a la sombra en Internet visitan varias páginas Web de múltiples proveedores de audio y luego determinan cuál de ellos tiene los precios más bajos. Esta política ordena a los diseñadores de sistemas instalar mecanismos que impidan a los agentes realizar estas comparaciones de precios. A pesar de que puede parecer una táctica violenta, en la realidad está bastante establecida en el ambiente empresarial físico. Por ejemplo, los abastos a menudo impiden que empleados de otros negocios caminen por los pasillos recopilando información sobre los precios. En algunos casos se puede generalizar esta política para que limite cualquier actividad externa de recopilación de información que pueda dar una ventaja competitiva a terceros. La palabra "significativa" en la política es deliberadamente ambigua, permitiendo que los sistemas informáticos evolucionen con los cambios. Esta política es muy útil dentro de una organización que ofrece numerosos productos o servicios a distintos precios.

Políticas Relacionadas: "Restricciones a la Recopilación de la Información"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Manejo de Información Sensible

Política: Toda divulgación a terceros de información secreta, confidencial o privada perteneciente a la Empresa X, debe estar acompañada de una declaración explícita que describa exactamente cuál información está restringida y cómo puede o no ser utilizada.

Comentario: Esta política se puede utilizar para atender asuntos relativos a la diseminación secundaria y el manejo no autorizado de la información restringida al salir de la Empresa X. Una declaración explícita puede formar parte de un acuerdo de confidencialidad firmado por un tercero que recibe la información o simplemente se puede exponer en forma narrativa o verbal en el momento de la divulgación. Algunas organizaciones agregan la palabra "escrita" a la política entre las palabras "declaración explícita". Unas simples instrucciones verbales pueden ser suficientes si el receptor ha firmado un acuerdo de confidencialidad con la Empresa X o si mantiene una relación de negocios de larga data con la Empresa X. La intención de esta política es básicamente requerir a aquellos que divulguen información confiable que suministren instrucciones

específicas sobre su manejo apropiado. Esta política asume que los términos "secreto, confidencial o privado" ya han sido definidos.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Diseminación Secundaria de la Información Secreta"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

10. Recepción de Información de Terceros

Política: Si un agente, empleado, consultor o contratista debe recibir información secreta o confidencial de un tercero a nombre de la Empresa X, esta divulgación debe estar precedida por la firma del tercero de un documento donde libera dicha información, autorizado por el departamento legal de la Empresa X.

Comentario: Esta política evita que la Empresa X se vea obligada a pagar regalías u otro tipo de compensación a terceros si introduce al mercado un producto que esté relacionado con las ideas divulgadas por un tercero. Este documento de liberación hace constar que la Empresa X no se encuentra bajo ninguna obligación de pagar regalías o compensaciones y que la recepción de la información no implica un acuerdo contractual. Esto puede ser un asunto particularmente difícil si la Empresa X ha desarrollado información similar en secreto. En este caso, la Empresa X puede determinar la naturaleza de la información a recibir y luego decidir no aceptarla para que no se presente ninguna discusión. Algunas organizaciones como las de capital a riesgo se preocupan tanto por esto que no firman, sin excepción, acuerdos de confidencialidad con otras personas. Es necesario consultar al departamento Legal de la Empresa X antes de elaborar una política de esta naturaleza.

Políticas Relacionadas: "Entrega de Información Secreta"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

11. Sistemas de Terceros Conectados a la Red

Política: Para tener acceso a la red de computadores de la Empresa X, todo tercero debe asegurarse de que sus propios sistemas están conectados de manera consistente con los requisitos de la Empresa X, inclusive, sin limitantes, del derecho a auditar sin previo aviso las

medidas de seguridad de aquellos sistemas conectados y el derecho a terminar de inmediato las conexiones de todos los sistemas de terceros.

Comentario: Esta política informa a los terceros con acceso a la red de la Empresa X que deben mantener la seguridad de sus propios sistemas para poder continuar trabajando con la red de la Empresa X. Es importante tener la capacidad de eliminar en forma inmediata una conexión que pudo haber sido explotada por un hacker, ya que éstos utilizan distintos sistemas para esconder sus huellas. Esta política intenta resolver el problema creciente de conciliar distintas políticas de seguridad en redes diferentes. La política brinda a los terceros una manera relativamente fácil de mantener un nivel de seguridad consistente ya que cuando están conectados a la red de la Empresa X, un sistema independiente cumple los requisitos de seguridad de la Empresa X, pero después que esta conexión termina la misma máquina se puede conectar a la red de otra organización y utilizar un grupo de controles distintos. Algunas organizaciones pueden incluir ejemplos específicos de sus tratos con terceros en este sentido.

Políticas Relacionadas: “[Interconexión de Sistemas](#),” “[Conexiones a Redes de Terceros](#),” y “[Conexiones en Red con Organizaciones Externas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Convenios con Terceros

Política: Todo convenio que se relacione con el manejo de información de la Empresa X por parte de terceros, debe incluir una cláusula que autorice a la Empresa X a auditar periódicamente los controles utilizados en las actividades en las cuales se maneja la información, y que especifique la manera en que se protege la información de la Empresa X.

Comentario: Esta política evita que los empleados de la Empresa X cedan inadvertidamente sus responsabilidades sobre la protección de la información de la Empresa X. Esto puede ocurrir cuando una organización externa se hace cargo de las operaciones de procesamiento de datos. Aún cuando la Empresa X decida que contratistas u otras organizaciones manejen las actividades de seguridad informática, siempre debe retener el derecho a especificar los requisitos para la protección de la información y el derecho a cerciorarse que los terceros los cumplen. Esta política está

redactada de tal manera que se puede realizar una auditoría por humanos o a través de herramientas automatizadas para auditorías.

Políticas Relacionadas: “[Responsabilidades de Terceros en la Seguridad Informática](#),” “[Aprobación de Contratos Externos](#),” y “[Términos y Condiciones para el Acceso de Terceros](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

13. Medidas de Seguridad en Organizaciones de Terceros

Política: Antes de otorgarse un identificador de usuario a un tercero, éste debe presentar evidencia documentada de la existencia de un sistema o proceso de seguridad informática, la cual debe ser aprobada por la gerencia de Seguridad Informática de la Empresa X, y el tercero debe convenir por escrito en resguardar dicho sistema o proceso para evitar el uso no autorizado o inapropiado de los sistemas de la Empresa X.

Comentario: Esta política reconoce y maneja los riesgos asociados con el acceso de terceros a los sistemas internos de la Empresa X. A menos que los terceros tengan y mantengan medidas confiables de seguridad informática, pueden ocurrir dos problemas. Personas sin autorización pueden tener acceso a los sistemas internos de la Empresa X y terceros autorizados pueden utilizar el acceso otorgado para fines incorrectos. Esta política exige que sea presentada evidencia documentada de la existencia de medidas de seguridad informática antes de que sea otorgado el identificador de usuario. Esta política también especifica que las medidas de seguridad informática deben ser constantemente observadas y que este requisito debe estar por escrito. Adicionalmente, esta política presenta a la gerencia interna de la Empresa X evidencia escrita de que se hizo una revisión del tercero con diligencia y esto puede ser utilizado luego en tribunales si se presenta un problema de seguridad que involucre al tercero. Esta política está dirigida a organizaciones más que a personas. En aquellos casos en que el tercero es una persona, se le entrega una lista de requisitos mínimos de seguridad para que convenga, por escrito, que se va a regir por ellos. Esta política es similar a la práctica en la cual los terceros deben presentar evidencia documentada de que pueden y van a proteger la información a punto de ser divulgada, antes de que se divulgue.

Políticas Relacionadas:“Identificadores Personales de Usuario — Responsabilidad”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

14. Política de Seguridad del Tercero

Política: Antes de divulgarse cualquier información propia de la Empresa X a un tercero, éste debe firmar un acuerdo de confidencialidad con la Empresa X y someter una copia de su política de seguridad informática a la consideración de la gerencia de Seguridad Informática de la Empresa X.

Comentario: Esta política garantiza que la información propia no será divulgada a terceros que no puedan protegerla adecuadamente. Se trata no sólo de exigir confidencialidad, ya que eso es práctica establecida, sino exigir que los terceros presenten su política de seguridad informática a la consideración de la gerencia de Seguridad Informática. En este caso, Seguridad Informática debe asegurarse de que el tercero tiene un sistema de control que garanticé la protección adecuada de la información propia de la Empresa X. Si Seguridad Informática no está satisfecha con la política, entonces la petición debe ser rechazada. Si se trata de agencias gubernamentales, la palabra "propia" puede ser reemplazada por la palabra "secreta". Esta política se dirige a organizaciones de terceros en vez de personas. Si una persona es considerada receptora de información propia, la Empresa X puede preparar una lista de requerimientos mínimos y esta persona puede acordar de forma escrita regirse por estos requerimientos mínimos.

Políticas Relacionadas:“Medidas de Seguridad en Organizaciones de Terceros”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

15. Información Recopilada Externamente

Política: Todo contrato con una organización externa, con un programador contratado o cualquier otra organización externa que maneje sistemas informáticos o los sistema de comunicación de la Empresa X, debe estipular que toda la información recopilada sobre la Empresa X será entregada al momento que ésta lo requiera, sin costo adicional.

Comentario: Esta política está fundamentada en varios intentos recientes de proveedores por "atrapar" a sus clientes. Por ejemplo, una organización que haga mantenimiento de equipos de sistemas informáticos puede guardar registros detallados y luego negarse a presentar estos registros a la empresa. Esta negativa crea problemas para la empresa cuando quiera realizar la actividad internamente al igual que cuando quiera cambiar de organización externa. Este tercero hace que salir de él sea costoso y lento. Esta política sigue la práctica general de las compañías de teléfono mediante la cual suministran la lista de los números discados, los patrones de llamadas a diferentes partes del mundo e información similar a la empresa que paga la factura. Esta política es una de muchas formas que las compañías pueden utilizar para protegerse contra la explotación por terceros que les niegan el acceso a su propia información. A esta política se puede agregar que la información sea devuelta en formato legible y que utilice convenciones comunes de archivado. Eso evita que un tercero presente la información en un formato que no se pueda utilizar.

Políticas Relacionadas:“Acceso del Cliente a Información Personal” y “Acceso a la Información Personal”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

16. Responsabilidades de Terceros en la Seguridad Informática

Política: Todo socio, distribuidor, cliente y asociado de la Empresa X debe estar consciente de sus responsabilidades en la seguridad informática a través de la inserción de lenguaje específico en los contratos que definen su relación con la empresa.

Comentario: Esta política establece claramente que la gerencia debe tomar en cuenta la asignación de responsabilidades en seguridad informática cuando hace cierra contratos con terceros. Estos temas no sólo deben ser considerados sino que, además, los contratos deben incluir los detalles específicos sobre la forma en que se manejarán. Un buen ejemplo de esto son los tratos que la gerencia cierra sobre gestión de instalaciones, donde un tercero toma el mando de las operaciones de tecnología informática de una organización. Las empresas a menudo olvidan o ignoran la seguridad informática cuando se trata de estas negociaciones, lo que trae como resultado su deterioro. Cuando la empresa plantea el reclamo ante la organización externa, ésta simplemente señala que el contrato no exige

mantener un nivel de seguridad y que la empresa debe pagar más si quiere servicio extra. En este ejemplo se asume que no ha ocurrido ningún problema grave. La política igualmente se aplica a otros ambientes tales como el uso por parte de un tercero de un servicio de red con valor agregado. Acerca de este tema tan importante debe consultarse a un consejero legal interno.

Políticas Relacionadas: “Convenios con Terceros,” “Convenios de Software con Terceros,” “Cumplimiento de Seguridad Informática,” “Servicios de Protección de Mensajes en Red,” “Sistemas de Terceros Conectados a la Red,” y “Adiestramiento Multidisciplinario”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

17. Devolución de la Información por el Personal Contratado

Política: Cuando un contrato termina o expira, todos los contratistas, consultores y temporales deben entregar a su gerente de proyecto todas las copias de la información perteneciente a la Empresa X recibida o creada durante la ejecución del contrato.

Comentario: Esta política establece que los contratistas, consultores y temporales deben devolver toda la información que recibieron para ejecutar el contrato. La propiedad de la información creada durante la ejecución del contrato puede ocasionar un conflicto, a menos que se haya especificado en el contrato. En ausencia de un convenio formal escrito, las cuestiones legales, como por ejemplo el hecho de que el trabajo fue un "trabajo a destajo", pueden controlar quién posee la propiedad real. La palabra "propiedad" se refiere a la propiedad legal, no al papel que cumple el Propietario de la información.

Políticas Relacionadas: “Derechos de Propiedad”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

18. Cumplimiento de Seguridad Informática

Política: Los consultores externos, los contratistas y los temporales externos deben estar supeditados a los mismos requisitos y tener las mismas responsabilidades en materia de seguridad informática que los empleados de la Empresa X.

Comentario: Esta política establece claramente quiénes deben acatar los requisitos de seguridad informática, tales como las políticas, las normas y los procedimientos. Esta política informa a los gerentes de niveles inferiores que deben suministrar a los consultores, contratistas y temporales la información necesaria para que entiendan cómo se hacen las cosas en la organización. Esta política también solicita de la gerencia no utilizar consultores, contratistas o temporales como medio para evitar los requisitos de seguridad exigidos a los empleados. Con esta política se expresa la noción universal de que los controles deben aplicarse a todas las personas en todos los ambientes de computación. Por ejemplo, toda persona debe portar un distintivo cuando está dentro de un edificio seguro. Muchas personas consideran que ciertas actividades privilegiadas o de gran confianza, como la administración de la seguridad de los sistemas, deben reservarse solamente para los empleados.

Políticas Relacionadas: “Fianzas de Trabajadores” y “Responsabilidades de Terceros en la Seguridad Informática”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4.03 Contratos Externos de Servicio

4.03.01 Requerimientos de Seguridad en Contratos Externos de Servicio

1. Reportes Independientes Sobre Controles

Política: Todo convenio hecho con organizaciones externas de sistemas informáticos debe estipular que la Empresa X recibirá anualmente un reporte que exprese una opinión independiente sobre la aceptabilidad de los controles en uso en la organización externa.

Comentario: Esta política evita que la gerencia interna establezca un convenio con una organización externa de servicios, a menos que sea incluido en el contrato que la organización presente reportes anuales e independientes de la revisión de los controles. Esto es una revisión independiente de las políticas, procedimientos y otros controles en la que se verifica si se mantienen normas de debido cuidado con los controles. Estos reportes pueden

ser presentados por organizaciones de contabilidad, aunque no necesariamente, y brindan a los clientes la certeza de que la organización externa se encarga satisfactoriamente de la seguridad. Estas auditorías no son financieras, sino de controles internos. A menudo los clientes no poseen la experticia suficiente para realizar estas auditorías a las organizaciones externas aún cuando éstas lo autoricen; por lo tanto, es más eficaz que la propia organización externa contrate a terceros para que realicen estas auditorías y no que cada cliente envíe a personas que se encarguen de esto, lo cual a su vez ahorra dinero al cliente.

Políticas Relacionadas:“Situación Financiera de Contratista Externo” y “Aprobación de Contratos Externos”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

2. Software del Proveedor de Servicios de Aplicaciones

Política: Todo proveedor de servicios de aplicaciones que maneje información de producción de la Empresa X debe licenciar el software a la Empresa X, depositar periódicamente en garantía la versión más reciente del código y suministrar documentación actualizada y detallada de los procedimientos.

Comentario:Esta política garantiza que si un proveedor de servicios de aplicaciones (ASP, por sus siglas en inglés) se declara en bancarrota o no quiera o no pueda cumplir con su contrato, la Empresa X continuará usando la aplicación externa. Con esta política se trata de influir en la negociación de nuevos contratos o la renegociación de los que ya existen. Esta política está relacionada sólo con los sistemas de aplicación que contienen una lógica de negocios única y rutinas difíciles de recrear. Las mismas consideraciones no se aplican por lo general a sistemas de software tales como el software de cortafuego, debido a que el paquete de un vendedor puede ser reemplazado por el de otro, aun cuando el alcance de la política puede expandirse para incluir software de sistemas únicos. No es suficiente poseer el código y tener derecho a utilizarlo, también es necesario que una organización tenga la documentación y procedimientos operacionales. Lo ideal es que el ASP adiestre al personal cliente sobre cómo utilizar el

software de aplicación, ya que es posible que la documentación no sea comprensible. El contrato con el ASP debe incluir una provisión para que la organización que adopte esta política tenga el derecho de ejercerla internamente si el ASP no le es satisfactorio. Además, será necesario un plan de conversión y de contingencia.

Políticas Relacionadas:“Planes de Recuperación Ante Desastre Computacional”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

3. Proveedor Alternativo de Procesamiento

Política: En todos los casos donde una organización externa maneja información crítica sobre los sistemas informáticos de producción de la Empresa X, un proveedor alterno debe estar preparado para tomar el control de inmediato, en el caso que la organización externa no sea capaz o no deseé cumplir con su contrato.

Comentario:Esta política reduce la vulnerabilidad que existe en la contratación de una organización externa para el manejo de actividades críticas de los sistemas informáticos. Esta política es bastante estricta ya que requiere la disponibilidad en todo momento de un proveedor alterno, lo cual la convierte en una política de planificación de contingencias. La motivación tras esta política son los numerosos casos donde organizaciones externas han dejado el negocio abruptamente, sin previo o muy poco aviso, dejando a sus clientes sin asistencia de conversión, y buscando un proveedor alterno. Encontrar un proveedor alterno implica realizar el procesamiento internamente, ya que no hay nada en la política tal como está escrita que evite esto. Esta política cubre, además de las situaciones donde el proveedor es incapaz de mantener sus compromisos contractuales, los casos de disputa en los que el proveedor primario deja de prestar los servicios ofrecidos. Esta política da por sentado que la palabra "crítica" se ha definido formalmente en otra política. Normalmente hay varios niveles críticos en los sistemas de aplicación.

Políticas Relacionadas:“Planes de Respuesta Ante Emergencias Computacionales”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

4. Planes de Contingencia para Proveedores de Servicios

Política: Todos los contratos con organizaciones para hospedaje de páginas Web, proveedores de servicios de aplicaciones, proveedores de seguridad para sistemas y otras organizaciones externas de sistemas informáticos deben incluir tanto un plan documentado de respaldo como un cronograma de pruebas periódicas de terceros.

Comentario: Esta política establece una medida de control mínima o un plan de respaldo que no se incluye a menudo en un contrato escrito. Si este requerimiento se incluye en un contrato, y la organización encargada no cumple, entonces hay un recurso legal y una organización suscrita está en capacidad de recuperar los daños. Cualesquier sean las palabras en el contrato, hay que ser diligentes y revisar periódicamente los planes de respaldo para asegurarse que funcionan correctamente. Un suscriptor a una organización de servicios de hospedaje para sitios web puede desear retener un consultor para que realice estas pruebas. Es posible que las organizaciones pequeñas no tengan influencia para cambiar los términos del contrato con la organización encargada. Sólo porque una organización encargada es grande no significa que hará un buen trabajo en cuanto a la estrategia de respaldo, procesos o planes de contingencia. En términos más generales, todo suscriptor debe establecer y mantener al día un plan de contingencia que utilice dichas medidas para probar su viabilidad, como por ejemplo, crear un negocio en Internet utilizando otra organización para hospedaje de sitios web.

Políticas Relacionadas: “[Compromiso en Acuerdos de Confidencialidad](#)” y “[Convenios con Terceros](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

5. Planes para el Retorno de Sistemas de Producción Manejados por Terceros

Política: Se debe preparar un plan de retorno eficaz, autorizado por la gerencia de Seguridad Informática y probarlo regularmente, que permita a la Empresa X realizar sus procesos internamente, antes que cualquier procesamiento de sistemas informáticos de producción se transfiera a una organización externa.

Comentario: Esta política garantiza que la Empresa X puede traer de vuelta a casa los procesos de producción que se encuentren en una organización externa cuando sea necesario. Un plan de retorno normalmente cubre temas como el reformato de los datos, la obtención de una versión actualizada del software utilizado para el

procesamiento y la búsqueda de la pericia necesaria para ayudar con operaciones computacionales. Muchas organizaciones que tienen actividades de sistemas informáticos en manos de organizaciones externas se dan cuenta que no cuentan con personal competente para dirigir las actividades relacionadas con el procesamiento interno. Están a merced de las organizaciones externas y por lo tanto deben aceptar los incrementos en los precios, términos contractuales no deseados en el momento de renovar un contrato y otras situaciones que en otras circunstancias no tolerarían. Tener planes de retorno actualizados coloca a la Empresa X en una posición donde puede volver a realizar sus procesos internamente. Esta política garantiza que la Empresa X negocie contratos que le permitan realizar sus procesos internamente en caso de que amerite hacerlo, como por ejemplo, si la organización externa no logra cumplir con el nivel de servicio acordado.

Políticas Relacionadas: “[Planes de Contingencia en Conversión de Software](#)” y “[Reversión a Procedimientos Manuales](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Cortafuegos y Servidores Compartidos Externamente

Política: La Empresa X no permite que su información interna esté contenida o sea procesada por un cortafuego, servidor u otro computador compartido con otra organización externa.

Comentario: Esta política evita situaciones en las cuales un computador compartido con otra empresa causa problemas de seguridad informática o de relaciones públicas. Si un computador es compartido, el personal de otra organización es capaz de acceder a información ubicada en el mismo, aun cuando no tengan privilegios de acceso autorizados que les permitan ver información de la Empresa X. Algunas organizaciones han recibido mala publicidad al divulgarse que compartían computadores con compañías menos reputadas, y aún cuando estas organizaciones no saben con quienes comparten los computadores de las organizaciones externas, son percibidas como culpables por asociación. Esta política es implementada específicamente para los sistemas diseñados bajo el principio de aislamiento que dice: “en la medida que varios componentes puedan ser aislados, generalmente su seguridad será mayor”.

Políticas Relacionadas: “[Consumo Excesivo de Recursos](#)” y “[Servidores para Aplicaciones Críticas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

7. Acceso a la Información Manejada por Contratista Externo

Política: IEn cada caso donde la Empresa X utilice una organización externa para procesar o manejar su información de producción, el contrato con dicha organización debe estipular claramente la entrega diaria a la Empresa X de una copia legible por computador de su información, o que la Empresa X tiene el derecho a obtener una copia legible por computador de su información, en cualquier momento y sin limitaciones.

Comentario:Esta política enfrenta y evita una táctica utilizada por los proveedores de servicio de aplicaciones y otras organizaciones externas, que consiste en retener los datos de producción hasta que el cliente haya pagado sus facturas o resuelva la disputa de forma conveniente para la gerencia de la organización externa. Mientras una disputa permanezca sin resolverse, el cliente de la organización externa se encuentra en severos inconvenientes e incluso puede quebrar debido a que no puede llevar a cabo sus actividades de negocios normalmente. Esta política está por lo tanto dirigida a evitar que la Empresa X llegue a algún convenio con las organizaciones externas que le impidan obtener la versión más reciente de su información de producción. No es suficiente la copia de la información, sino que debe estar en formato legible parecido al que utiliza la Empresa X u otra organización externa. Esto último debe estar estipulado en la política pero está implícito en las palabras "legibles por computador". Con esta política se asume que el término "producción" ha sido definido como datos utilizados de apoyo para la actividad regular y recurrente de negocios.

Políticas Relacionadas:["Planes de Contingencia para Proveedores de Servicios"](#)

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

8. Decisiones Sobre Control de Acceso

Política: Las decisiones referentes a quiénes tendrán acceso a la información y los sistemas informáticos de la Empresa X deben ser tomadas únicamente por la gerencia de la Empresa X.

Comentario:Esta política evita que la gerencia interna delegue sus responsabilidades. En algunas organizaciones la gerencia opta por entregar todo lo relativo al manejo de sistemas informáticos a una o más organizaciones externas. Mientras que la seguridad administrativa, el monitoreo y detección de intrusos en la red y otras tareas de seguridad informática pueden ser delegadas a una organización externa, las decisiones referentes al acceso a sistemas informáticos no deben ser delegadas, ya que delegar una decisión tan crítica y esencial sería ir en contra de las normas que establecen que dichas decisiones se deben reservar para la gerencia interna. Nada de lo contenido en esta política impide que la gerencia utilice a organizaciones externas o de consultoría para recibir recomendaciones sobre cómo definir los privilegios de acceso.

Políticas Relacionadas:["Propiedad de la Información"](#) y ["Delegación de la Propiedad de la Información"](#)

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

9. Aprobación de Contratos Externos

Política: Todos los contratos que estén relacionados con los sistemas informáticos deben ser revisados y autorizados por la gerencia de Seguridad Informática, que es responsable de garantizar que dichos contratos definen adecuadamente las responsabilidades de seguridad informática, cómo responder a una eventual variedad de problemas de seguridad y el derecho a terminar el contrato si se puede demostrar que la organización externa no cumple con los términos de seguridad informática establecidos en el contrato.

Comentario:Esta política asigna claramente las responsabilidades de examinar los contratos externos para garantizar que sean suficientemente explícitos y claros en el área de seguridad informática. En muchos casos, la organización que contrató a una organización externa no toma en cuenta la definición de responsabilidades de seguridad y procedimientos para la resolución de los problemas. Como resultado, cuando ocurre un problema de seguridad, la organización externa puede disminuir sus esfuerzos porque no es recompensada ni castigada con base en la seguridad informática. Esta política cambia esta actitud, dándole a la organización mecanismos legales, como la terminación de contrato, que pueden ser utilizados para que la organización externa tome en serio el tema de la seguridad. La política tiene como propósito evitar las situaciones donde el departamento de Seguridad Informática sólo revisa los convenios externos cuando hay problemas. La

revisión de los contratos es responsabilidad última del departamento Legal, y la política puede ser diseñada para incluir tal referencia.

Políticas Relacionadas: “Delegación de la Propiedad de la Información,” “Convenios con Terceros,” y “Resolución de Problemas de Seguridad Informática”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

10. Situación Financiera de Contratista Externo

Política: Todas las organizaciones externas de sistemas informáticos que sean contratadas para encargarse de la información de producción de la Empresa X deben presentar declaraciones financieras trimestrales.

Comentario: Esta política afecta la negociación de nuevos contratos o la renegociación de contratos ya existentes con organizaciones externas de sistemas informáticos. Si una organización externa está poco dispuesta a revelar información financiera, esto se puede tomar como un mal indicio de que está en peligro de salirse del negocio. Un cese de servicios no anticipado y no informado tiene repercusiones serias y hasta fatales para los clientes de una organización externa. La industria de sistemas informáticos es notoriamente volátil y varias organizaciones externas han quedado fuera del negocio de la noche a la mañana sin advertencia alguna. Esta política es una advertencia temprana para la gerencia de clientes externos. Sólo recibir declaraciones financieras no es suficiente y por ello es necesario acompañar esta política con otras adicionales.

Políticas Relacionadas: “Condición Financiera de Proveedores Importantes” y “Planes de Recuperación Ante Desastre Computacional”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Procesos de Producción Manejados por Compañías Extranjeras

Política: La gerencia de la Empresa X no debe entregar ningún aspecto del manejo de los sistemas informáticos de producción, inclusive sin limitantes, del diseño de sistemas, desarrollo, pruebas, operación y mantenimiento, a una organización externa que tenga su sede en un país extranjero o que pertenezca a una empresa extranjera.

Comentario: Esta política garantiza que los problemas con las organizaciones externas serán mínimos. A pesar de ser más económico, el uso de organizaciones externas extranjeras es más problemático, lo que puede afectar la confiabilidad del sistema, su seguridad y la integridad de los datos. Más allá de las barreras del lenguaje, el personal de la Empresa X puede no ser capaz de inspeccionar las instalaciones de organizaciones externas extranjeras, ni demandar en tribunales domésticos si hay disputas, ni tener la capacidad de confiar en el hecho de que la organización externa esté sujeta a las mismas leyes que la Empresa X. Durante la entrega de los procesos de producción a una compañía externa extranjera, a menudo se presentan problemas de comunicación que pueden empeorar por las diferencias culturales. Las empresas extranjeras pueden retirarse del mercado con una mínima advertencia pública o de acuerdo a criterios de negocios diferentes a los de las empresas domésticas. Como resultado, a la Empresa X se le hace más difícil anticipar cuándo dejarán de estar disponibles los servicios de una organización externa extranjera.

Políticas Relacionadas: “Garantía Especial de Software” y “Compromiso en Acuerdos de Confidencialidad”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

5 CLASIFICACIÓN Y CONTROL DE ACTIVOS

5.01 Responsabilidad por Activos

5.01.01 Inventario de Activos

1. Clasificación del Software y los Sistemas

Política: Seguridad Informática debe preparar anualmente una lista del software y de los sistemas desarrollados internamente, que puedan dar ventaja competitiva a la Empresa X.

Comentario: Esta política exige a la gerencia de Seguridad Informática o a los coordinadores locales de seguridad informática examinar periódicamente la importancia del software y los sistemas desarrollados internamente. La lista debe utilizarse como un mecanismo para garantizar que el software y los sistemas informáticos sean clasificados apropiadamente según un esquema de clasificación de datos internos. De igual manera, la lista debe ser utilizada para determinar si los controles asociados son adecuados, garantizando así a la organización que sus recursos de información máspreciados son protegidos adecuadamente. Esta política es relevante para aquellas organizaciones que han desarrollado un software único, sistemas expertos, sistemas de manejo de conocimiento y otros materiales que les dan ventaja competitiva. Esta política puede ser utilizada como un reporte que refleje cómo utilizan sus sistemas informáticos para alcanzar una ventaja competitiva. En este sentido, puede ser apropiado que Seguridad Informática trabaje con el departamento de Planificación Estratégica o el grupo de Arquitectura de Sistemas dentro del departamento de Seguridad Informática. En algunas organizaciones, la identificación de materiales que brindan ventaja competitiva puede hacerse por un grupo de manejo o almacenamiento de datos.

Políticas Relacionadas: “[Planes de Seguridad Informática](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Inventario de Activos — Tecnología

Política: La gerencia de Seguridad Informática debe preparar un inventario anual de los sistemas informáticos de producción detallando todo el hardware existente en producción, el software y los enlaces de comunicación.

Comentario: Esta política requiere que la gerencia prepare un inventario anual del hardware, software y los enlaces de comunicación de los sistemas informáticos de producción. Una organización puede planificar apropiadamente para los desastres si conoce los componentes de los sistemas existentes. En muchas organizaciones los sistemas informáticos cambian tan rápidamente que un inventario actualizado es una herramienta valiosa no sólo para planes de contingencia. Por ejemplo, un inventario actualizado es útil para la gerencia que esté negociando un convenio de compras por volumen con un proveedor de software. De igual manera, el inventario es útil para las actividades de seguridad informática, tales como determinar cuales computadores personales están protegidos por un software antivirus. Debido a que las redes de área local y otros sistemas distribuidos de computación a menudo no están bien documentados, esta política es particularmente útil para redes de área local, sistemas cliente-servidor, y sistemas de oficina automatizados. Cuando las máquinas están conectadas a una red local, productos de software pueden realizar un inventario del hardware y software de los computadores personales. Si no está disponible un inventario del sistema de producción entonces será útil un inventario del equipo para aplicaciones críticas para fines de planes de contingencia. Esta política implica lo que se conoce como inventario periódico, en contraposición al inventario continuo.

Políticas Relacionadas: “[Control de Inventario](#)” y “[Puestos Técnicos Esenciales](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Control de Inventario

Política: Los Custodios de los equipos de la Empresa X deben mantener un control continuo de inventario, un registro del nuevo Custodio y la nueva ubicación de todo el equipo suministrado a otros, además de la seguridad física del equipo.

Comentario: A medida que aumenta la distribución de los equipos de sistemas informáticos, mayor necesidad hay de confiar en el personal de base para proteger y dar cuenta de estos equipos. Una manera de hacer esto es a través de los Custodios de los equipos, que no deben ser confundidos con los Custodios de la Información. Los Custodios de Equipos hacen un seguimiento a los equipos en las oficinas, en las casas o en laboratorios de computación. Si una organización designa Custodios de equipos, y tiene constancia escrita que respalden esas designaciones, tendrá menos problemas en discusiones sobre la propiedad del equipo al momento de terminar una relación de trabajo. Los Custodios también son útiles en el control e identificación de equipo robado. La existencia de los inventarios de equipos también ayuda en los planes de contingencia, en los esfuerzos para mejorar los equipos y en el esfuerzo por lograr un reembolso del seguro por la pérdida de equipos. Las palabras "inventario continuo" contrastan con "inventario periódico", haciéndose necesario definir ambos términos en algunas instancias de manera explícita a los Custodios de los equipos. Esta política puede ser modificada para que los Custodios de equipos puedan salvaguardar sus constancias de inventarios contra una alteración no autorizada con la que se trate de ocultar un robo.

Políticas Relacionadas: “[Responsabilidades del Custodio de la Información](#),” “[Inventario de Activos — Información](#),” e “[Inventario de Activos — Tecnología](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Diccionario de Datos

Política: Todo tipo de información nueva de la Empresa X, creada y utilizada en las operaciones de negocios del día a día, debe estar reflejada en el diccionario corporativo de datos.

Comentario: Esta política indica a los trabajadores que el diccionario corporativo de datos debe reflejar todo tipo de información utilizada en el día a día de las operaciones de producción. A través del diccionario corporativo de datos, la gerencia puede conocer la información operacional más importante dentro de la organización. Pueden censurar la información rápidamente donde se necesite y aplicar controles adicionales a aquellas informaciones que requieran dichos controles. Esta política toma una perspectiva orientada hacia el conocimiento de la información por la gerencia en vez de enfocarse en la censura y asume que si la gerencia conoce todos los tipos de información disponi-

bles dentro de la organización, estará más capacitada para controlar dicha información. Si la gerencia desconoce la información existente no puede manejarla apropiadamente.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” y “[Sistemas Secretos](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Procura de Hardware y Software

Política: Todo el hardware y software debe obtenerse a través del departamento de Compras de acuerdo con las normas de compatibilidad IT de la empresa.

Comentario: A menudo los usuarios desechan los canales normales de compra para obtener más rápido el software o hardware o para evitar tener que cumplir normas técnicas internas. Esta práctica les permite comprar hardware y software que, sin saberlo, compromete la seguridad de los sistemas de red o de computación. Por ejemplo, pueden comprar un computador de escritorio que tenga una unidad para disco flexible cuando el equipo normal que utilizan no la tiene. Permitirles a los usuarios comprar independientemente crea un caos en el ambiente computacional en el cual los sistemas no tienen soportes, son inoperables entre ellos o incompatibles con la red. Esta política requiere que todas las compras se realicen a través de una unidad organizacional que siga de cerca las solicitudes para cumplir las normas técnicas internas. Cuando existan dudas acerca del cumplimiento, el departamento de Compras dirigirá una solicitud de seguridad informática relacionada con el hardware y software al departamento de Seguridad Informática para la autorización. La política puede ser redactada de tal manera que todas las compras pasen por el departamento de Tecnología de Información.

Políticas Relacionadas: “[Compra de Soluciones de Seguridad Informática](#),” “[Seguridad Informática Centralizada](#),” “[Sistemas de Computación Pertenecientes a Trabajadores](#),” y “[Liberación de Componentes Usados](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

6. Propiedad de la Información

Política: Cuando una unidad organizacional en particular posea o utilice la información de producción, debe tener designada un Propietario responsable de

determinar las clasificaciones correspondientes a la confidencialidad y la criticidad, tomar decisiones sobre quién tiene acceso a la información y garantizar que se utilizan los controles adecuados en el almacenamiento, manejo, distribución y uso regular de la información.

Comentario: Esta política garantiza que toda información de producción tiene un Propietario designado, y que éste está versado en lo relativo a seguridad informática. Mientras el Propietario no especifique cómo proteger la información de acuerdo a cierta clasificación, él asignará la clasificación y los controles adecuados entrarán en funcionamiento. De igual manera, el Propietario no especifica cómo respaldar o de alguna manera facilitar la continua disponibilidad de la información crítica. El grado de criticidad que el Propietario le asigne, implica la disponibilidad de los controles necesarios. Las decisiones sobre control de acceso a ser efectuadas por el Propietario incluyen los derechos para crear, modificar, eliminar, visualizar y utilizar la información. El Propietario especifica a cuál persona o grupo de personas se otorga privilegios de acceso. Generalmente el Propietario está muy ocupado y poco inclinado a lo técnico para involucrarse en los asuntos técnicos de seguridad a ser implantados. Sin embargo, hay una conexión crítica entre el manejo del negocio y la gerencia de sistemas informáticos y como tal, sus consideraciones deben determinar qué tipo de seguridad se va a aplicar. Algunas organizaciones querrán mencionar en su política que los Propietarios son generalmente departamentos usuarios y gerentes medios. Desde otro punto de vista, es difícil designar a los Propietarios si el inventario no se ha completado. Esto puede involucrar la compilación de un diccionario de datos o directorio de datos. En esta política se asume que la organización ha adoptado tanto la clasificación de confidencialidad como la jerarquía de criticidad.

Políticas Relacionadas: ‘‘Clasificación de Datos en Cuatro Categorías,’’ ‘‘Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,’’ ‘‘Delegación de la Propiedad de la Información,’’ e ‘‘Inventario de Activos — Información’’

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

7. Control de los Activos Informáticos

Política: La Gerencia debe asignar específicamente las responsabilidades por las medidas de control que protejan todo activo informático importante.

Comentario: Esta política garantiza que se ha asignado la responsabilidad de los controles que protegen los activos informáticos, tales como la base de datos de la información de contacto de los clientes. Algunas personas diferencian entre responsabilidad y quien responde por algo, pero esta política no lo hace. Esta política asume que los activos informáticos han sido identificados; por ejemplo, en un diccionario de datos que abarque toda la organización. La identificación de los activos informáticos también ocurre cuando se hacen evaluaciones de riesgos y cuando se preparan planes de contingencia. Al contrario de las políticas que se ocupan de la información de la propiedad, esta política se refiere a la asignación de la responsabilidad por los controles, no por la información misma. En muchos casos, la responsabilidad es asignada a aquéllos que trabajan como analistas de negocios, operadores de centros de datos, administradores de seguridad y administradores de redes. Es importante que la responsabilidad sobre los controles sea clara y esté asignada de manera definitiva, no importa quién sea el responsable, para que no haya fallas en el control. Los ‘‘activos informáticos’’ también pueden llamarse ‘‘recursos informáticos’’.

Políticas Relacionadas: ‘‘Inventario de Activos — Información,’’ ‘‘Inventario de Activos — Tecnología,’’ ‘‘Índices de Base de Datos Que Contienen Información Privada,’’ ‘‘Naturaleza y Ubicación de la Información de la Organización,’’ y ‘‘Custodio de la Información’’

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Administrador de Seguridad Designado

Política: Todo sistema computarizado multiusuario de la Empresa X debe contar con un administrador de seguridad designado para definir los privilegios de los usuarios, monitorear los registros del control de acceso y realizar actividades similares.

Comentario: Esta política garantiza que una persona específica es designada como responsable por la seguridad. Cuando no está claro quién es responsable por la seguridad, a menudo las tareas de seguridad son descuidadas y como resultado la organización se expone indebidamente a distintos problemas. Todos los sistemas multiusuario, incluyendo las estaciones de trabajo utilizados por más de una persona que manejen información confidencial, crítica o valiosa, deben ser protegidos por un sistema de control de acceso. A menudo esto incluye contraseñas fijas y otras tecnologías como tarjetas inteligentes, tarjetas de identificación y reconocimiento de huellas dactilares. Para los

propósitos de esta política, todas las redes computarizadas son sistemas multiusuario y como tales debe asignárseles uno o más administradores de seguridad. No se exige a los administradores de sistemas trabajar a tiempo completo y los que trabajan medio tiempo lo hacen en organizaciones pequeñas o en aquellos sistemas manejados por departamentos u otra unidad organizacional descentralizada. Por otra parte, esta política va tomando importancia en la medida en que los sistemas informáticos son distribuidos, como en el caso de las redes de área local, los computadores personales y los sistemas cliente-servidor.

Políticas Relacionadas: “[Actualización de Información de Producción](#)” y “[Enlaces de Seguridad Informática](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9. Administradores de Seguridad Suplentes

Política: Todo sistema multiusuario de la Empresa X con un sistema de control de acceso debe tener designado un empleado adiestrado como administrador de seguridad suplente, que lo pueda sustituir en caso de que el administrador principal no esté disponible.

Comentario: Esta política pretende evitar situaciones incómodas donde no exista un administrador de seguridad suplente, en cuyo caso el negocio puede ser afectado o interrumpirse. Si un administrador suplente está listo para sustituir al administrador regular entonces es poco probable que los sistemas de seguridad se vean comprometidos para continuar con el negocio. Ambos administradores deben ser empleados, porque son más leales y a menudo tienen más tiempo en la empresa que los contratistas, consultores o temporales. Esta política puede utilizarse para obtener personal necesario y recursos de adiestramiento. Esta política supone que las palabras "sistema de control de acceso" han sido ya definidas. Generalmente estas palabras significan un sistema de identificación del usuario con contraseñas fijas con controles asociados a los privilegios del usuario, pero hay muchas otras opciones disponibles, como las tarjetas de contraseñas dinámicas.

Políticas Relacionadas: “[Administrador de Seguridad Designado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Inventario de Activos — Información

Política: La gerencia de Sistemas Informáticos debe recopilar y actualizar anualmente un diccionario corporativo de datos y otras descripciones de alto nivel de los activos informáticos más importantes de la Empresa X.

Comentario: Esta política requiere que Sistemas Informáticos organice y documente información acerca de la información. Esta información, a menudo en forma de diccionario de datos o de directorio, es invaluable cuando se trata de planificar los proyectos futuras de desarrollo de aplicaciones, migrar aplicaciones de los mainframes a sistemas cliente-servidor y diseñar un sistema informático ejecutivo. Es también útil cuando se realizan las evaluaciones de riesgo y la preparación de planes de contingencia para los sistemas informáticos. El diccionario de datos puede ser utilizado por los auditores de tecnología de información para determinar si los controles se aplican consistentemente a la información, a todo lo largo de aplicaciones y de sistemas. Un diccionario de datos es esencial si la noción de Propietarios, Custodios y usuarios va a ser utilizada exitosamente dentro de una empresa en particular. Estas distinciones dependen de la habilidad para definir, ubicar, controlar y manejar información como sólo puede hacerse a través de un diccionario de datos u otra herramienta similar, ya que ayuda a las organizaciones a aceptar la complejidad de sus sistemas informáticos. Esta política es importante para las grandes organizaciones, aunque a las organizaciones medianas también les parecerá apropiada. Tampoco debemos olvidar que el control de acceso a los diccionarios de datos es esencial ya que no todos necesitan saber lo que contienen dichos diccionarios.

Políticas Relacionadas: “[Control de los Activos Informáticos](#),” “[Custodio de la Información](#),” “[Información Personal para el Funcionamiento del Negocio](#),” “[Sistemas Secretos](#),” “[Índices de Base de Datos Que Contienen Información Privada](#),” y “[Naturaleza y Ubicación de la Información de la Organización](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Seguimiento de Equipos

Política: Todos los computadores y equipos de comunicación de la Empresa X deben llevar un identificador único legible por el computador de manera que los inventarios físicos puedan hacerse de manera eficiente.

Comentario: Muchos departamentos de sistemas informáticos no saben con exactitud qué equipo poseen, o alquilan, o de algún modo controlan. Un inventario actualizado es una herramienta gerencial importante para tomar decisiones tales como si algún equipo ha sido robado, qué equipos necesitan mejorarse y para planificar re-configuraciones de red. Estos inventarios son útiles cuando se termina la relación de trabajo con el empleado, que en tales casos a veces degenera en disputa acerca del equipo que el empleado tuvo en su poder y cuáles de las piezas del equipo pertenecen al empleador. El "identificador único" mencionado en esta política puede ser un código de barra, una marca de reconocimiento óptico u otra marca sensible al computador. La marca debe ser invisible a simple vista para dificultar su remoción. Si no es factible tener un sistema de inventarios computarizados, se debe utilizar algún tipo de etiqueta física que se pueda rastrear. Esta política es importante para los inventarios de computadores personales, estaciones de trabajo, máquinas de fax y otros equipos de oficina pequeños.

Políticas Relacionadas: “Procedimiento de Control de Cambios” y “Revisión de los Convenios de Licencia del Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Códigos de Identificación de los Equipos

Política: Todos los computadores y equipos de comunicación de la Empresa X deben tener un número de identificación indeleble, grabado en el equipo para ayudar a la policía en sus intentos por devolver la propiedad robada.

Comentario: El robo y la reventa de computadores y equipos de comunicación se han convertido en un grave problema. Gran parte del equipo perdido y robado que se ha recuperado nunca se devuelve, puesto que no se sabe a quién pertenece. Se encuentran disponibles nuevas tecnologías para marcar el equipo, como el número del seguro social, un número telefónico u otro número único. Muchas de estas marcas son invisibles a simple vista para que los ladrones no traten de oscurecerlas. También pueden ser utilizadas en el futuro como información de las bases de datos que describen equipos robados. Esta política es importante especialmente para equipos portátiles, laptops y otros computadores personales portátiles, así como para el momento de finalizar la relación de trabajo cuando hay que determinar el propietario de una pieza de equipo.

Políticas Relacionadas: “Seguimiento de Equipos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5.02 Clasificación de la Información

5.02.01 Lineamientos para la Clasificación

1. Propiedad de Archivos y Mensajes

Política: La Empresa X tiene la propiedad legal del contenido de todos los archivos y mensajes almacenados o transmitidos en sus computadores y sistemas de redes, y se reserva el derecho de acceder a esta información sin aviso previo cuando exista una necesidad genuina de negocios.

Comentario: Esta política aclara el asunto de la propiedad de la información contenida en los sistemas de la Empresa X. Puede facilitar el examen de los archivos de correo electrónico y los directorios de archivos de computadores personales que los usuarios podrían de otra manera considerar confidenciales y privados. Puede actuar también con efecto disuasorio, desalentando a los usuarios a utilizar los sistemas de la Empresa X para fines personales. Indirectamente esta

política puede resolver disputas acerca de la propiedad del software escrito por los empleados, contratista o consultores. Las organizaciones usuarias pueden extender su alcance para incluir sistemas telefónicos, como los correos de voz. Algunas organizaciones pueden agregar el reconocimiento de que la Empresa X no tiene propiedad legal de la información guardada en custodia para un tercero, o del software o de otra información patentada o intelectual protegida obtenida de un tercero.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Herramientas de Monitoreo de Sistemas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Clasificación de Datos en Cuatro Categorías

Política: Todos los datos de la Empresa X deben ser divididos en las siguientes cuatro clasificaciones: SECRETA, CONFIDENCIAL, PRIVADA y NO CLASIFICADA. Deben establecerse procedimientos distintos para manejar, etiquetar y revisar cada clasificación

Comentario: Este sistema normal de clasificación de datos debe utilizarse en toda la Empresa X para asignar clasificaciones según los distintos requerimientos de manejo de acuerdo con la [Tabla 3-1](#). Esta política suministra información a todos los trabajadores para guiarlos en el manejo de la seguridad de la información sensible de la Empresa X. La designación de este conjunto de clasificaciones es apropiada para una organización mediana o grande que no tiene que ocuparse con información especialmente sensible, tal como información sobre defensa nacional. Organizaciones con muchos tipos de datos sensibles querrán añadir categorías adicionales para afinar el procedimiento para manejar la información. Más allá de las cuatro categorías mencionadas, a menudo existe una categoría para información "pública". Esto se aplica a la información que ha sido autorizada por la gerencia para su divulgación pública. La divulgación de información pública es consistente con la política y no impactará negativamente a la Empresa X, sus empleados, sus accionistas, socios de negocios o sus clientes. La categoría a ser utilizada de manera predeterminada, a falta de más información y por ser la más frecuente, es "no clasificada". Esta política puede comprimirse para que sólo se usen tres o incluso dos categorías. La mayoría de las políticas de clasificación de datos incluyen ejemplos específicos que ayudan a los empleados a distinguir entre categorías. Datos sobre salario son considerados "privados". Algunas organizaciones añaden palabras a la política que indican que los borradores de información deben ser clasificados y manejados de la misma manera que las versiones finales. La política presentada aquí puede hacerse más explícita, lo cual puede contemplar el cambio de las palabras "impacto negativo" con palabras como pérdida financiera, ganancia para los competidores, notable pérdida de confianza para la Empresa X o notable reducción de la posición de la Empresa X en la comunidad.

Tabla 3-1: Clasificación de Datos en Cuatro Categorías

SECRETA

Tabla 3-1: Clasificación de Datos en Cuatro Categorías

Se aplica a la información más sensible del negocio, cuyo propósito es estrictamente de uso interno de la Empresa X. Su divulgación no autorizada podría dañar seria y adversamente a la Empresa X, sus accionistas, socios o a sus clientes.
CONFIDENCIAL
Se aplica a la información de negocios menos crítica, pero aún importante para su uso en la Empresa X. Su divulgación no autorizada podría impactar negativamente a la Empresa X, sus accionistas, sus socios o sus clientes.
PRIVADA
Se aplica a información personal que se ha de usar en la Empresa X. Su divulgación no autorizada podría impactar seria y negativamente a la Empresa X y a sus empleados.
NO CLASIFICADA
Se aplica a cualquier otra información que no corresponda a las tres clasificaciones anteriores. Si bien su divulgación no autorizada va contra la política, no se espera que tenga un impacto serio o adverso sobre la Empresa X, sus empleados, accionistas, socios y clientes.

Políticas Relacionadas: ['Fecha de Desclasificación'](#), ['Revisión Anual de la Desclasificación'](#), ["Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones"](#), y ["Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad"](#)

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

3. Clasificación de Datos en Tres Categorías

Política: Toda la información de la Empresa X y toda la información confiada a ella por terceros corresponden a una de tres clasificaciones de sensibilidad.

Comentario: Este sistema de clasificación de datos debe ser utilizado en toda la Empresa X para asignar clasificaciones de sensibilidad según los distintos requerimientos de manejo, de acuerdo con lo establecido en la [Tabla 3-2](#). Esta política establece un esquema de clasificación de datos apropiado para una organización pequeña o mediana que no se ocupe de información sobre defensa nacional. Esta política es simple y concisa como parte del esfuerzo por minimizar costos. La intención de esta política es crear distinciones básicas

con las cuales pueden crearse otras políticas y reglas operacionales. Esta política combina dos filosofías básicas del control de acceso. Para la información más sensible utiliza el principio de la necesidad de conocer, y para la información menos sensible utiliza el principio de necesidad de retener. Se debe ejercer cautela ya que una vez que un sistema de clasificación de datos se adopta, es caro y difícil cambiarlo a otro sistema. La organización debe estudiar cuidadosamente sus necesidades antes de adoptar una política como ésta. Los sistemas de clasificación también se utilizan para la criticidad de los datos. Esta política asume que el término "Propietario de la Información" ya ha sido definido.

Tabla 3-2: Clasificación de Datos en Tres Categorías

CONFIDENCIAL
El acceso a esta información debe estar muy restringido de acuerdo con el concepto de necesidad de conocer. Su divulgación requiere la autorización del Propietario de la información y, en el caso de terceros, también un acuerdo firmado de confidencialidad. Los ejemplos incluyen las evaluaciones de desempeño de los empleados y los planes de desarrollo de nuevos productos.
USO INTERNO SOLAMENTE
Esta información debe divulgarse a terceros sólo si se ha firmado un acuerdo de confidencialidad. No se espera que su divulgación cause un serio daño a la Empresa X, y se brinda libre acceso a ella a los todos los trabajadores internos en la intranet de la organización. Los ejemplos incluyen la guía telefónica y los calendarios automáticos del personal. Esta es la clasificación predeterminada de cualquier información no específicamente designada.
PUBLICA
Esta información ha sido explícitamente autorizada por el departamento de Mercadeo o Relaciones Públicas como adecuada para su diseminación pública. Los ejemplos incluyen panfletos de mercadeo y las notas de prensa.

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” “Clasificación de Datos en Cuatro Categorías,” y “Propiedad de la Información”

Política Dirigida a: Todos

Ambientes de Seguridad: Bajos y medianos

4. Clasificación Cerrada de Datos en Dos Categorías

Política: Toda información de la Empresa X que no esté marcada específicamente como "autorizada para el conocimiento público" o que no es regular o repetidamente compartida con grupos externos, es confidencial y no debe ser compartida con grupos externos a menos que se obtenga la autorización del Propietario de la Información.

Comentario: Esta política hace la clasificación de datos fácil, económica y directa. La política dicta dos categorías de sensibilidad específicas para la información, y también especifica cuál de estas dos categorías se aplica cuando no hay marcas evidentes en la información. Esta política es en realidad muy común en los negocios pequeños porque es expedita y eficaz. Esta política supone que se han designado Propietarios de la información. Si la organización que adopta la política no tiene o no quiere adoptar Propietarios de la información, ésta puede modificarse para hacer referencia a un ejecutivo designado, por ejemplo, el director de Relaciones Públicas o el director Legal. Esta política asume que la organización adoptante no es una agencia gubernamental, porque una agencia civil gubernamental debe compartir mucha información con el público y esto hace que la política sea engorrosa y cara de administrar.

Políticas Relacionadas: “Clasificación Abierta de Datos en Dos Categorías,” “Mal Funcionamiento del Control de Acceso,” “Permisos Predeterminados de Archivo,” y “Restricción de Privilegios — Necesidad de Retener”

Política Dirigida a: Todos

Ambientes de Seguridad: Bajos y medianos

5. Clasificación Abierta de Datos en Dos Categorías

Política: Toda información de la Empresa X que no haya sido marcada específicamente como "confidencial" está autorizada para hacerse del conocimiento público y puede compartirse con grupos externos sin el permiso específico de la gerencia con la excepción de la información que está restringida por las leyes y los reglamentos.

Comentario: Esta política va dirigida a hacer la vida más fácil de los trabajadores que se preguntan cuál información pueden compartir con terceros. Esta política es generalmente apropiada para una agencia civil gubernamental, como una que recopile estadísticas

económicas sobre el trabajo y los negocios. El mayor problema de esta política es que se puede quitar la etiqueta a la información. Si un empleado está empeñado en sabotear la organización que adopte esta política, simplemente quita la etiqueta que dice que la información es confidencial y, así, la información pasa a ser apropiada para su diseminación sin más consultas a la gerencia. Esta es una política inusual que no suele funcionar para muchas organizaciones y por lo general no se recomienda.

Políticas Relacionadas: “Etiquetas Incorrectas de Clasificación de Datos,” “Uso de Derechos en Sistemas Informáticos,” y “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Todos

Ambientes de Seguridad: Bajos

6. Prefijos de Categorías de Clasificación de Datos

Política: Deben utilizarse prefijos, tales como "médico" o "financiero", delante de las categorías autorizadas de clasificación de datos.

Comentario: Esta política suministra mayor granularidad que la clasificación normal de datos. Si la información específica tiene que ver con los exámenes médicos del empleado, entonces la información debe ser etiquetada como "Médico—Privado". Sólo las personas que tratan cuestiones médicas de los empleados tienen acceso a esta información. Ante la falta de mayor información de acceso, simplemente etiquetando la información como "Privada" no es suficiente para restringir el acceso. Estos prefijos no confieren ninguna protección adicional a la suministrada por las marcas corrientes. En otras palabras, la información privada debe ser manejada de cierta manera, sin importar los prefijos. Los prefijos específicos están definidos en esta política u otras similares. Como alternativa, los prefijos pueden ser escogidos por los Propietarios de la información correspondientes. La segunda de estas alternativas corre el riesgo de confundir a las personas especialmente cuando se utilizan sinónimos y términos superpuestos.

Políticas Relacionadas: “Etiquetado de Clasificación de Datos” y “Clasificaciones de Medios de Almacenamiento de Datos”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

7. Declaración de Secreto Industrial

Política: El consejero legal principal de la Empresa X es la única persona autorizada para designar cualquier información de la Empresa X como secreto industrial.

Comentario: Esta política aclara que la designación de secreto industrial puede ser aplicada a cierta información sólo después de que el consejero legal principal haya realizado un análisis adecuado de las circunstancias. Se recomienda que los secretos industriales y la propiedad informática sean guardados celosamente, de manera que no se conozcan en toda la organización. Los secretos industriales deben probar su valor comercial, y la organización específicamente debe ser capaz de demostrar que este conocimiento exclusivo de un secreto industrial le ha permitido lograr una ganancia. Mientras que en términos generales estas ideas pueden ser comprendidas por cualquiera, tienen un número de matices que es mejor dejarlos a los abogados. La designación de cierta información como secreto industrial no interfiere de ninguna manera con la aplicación de etiquetas de clasificación de datos, tales como secreto. Esta política no impide que el Propietario de la información designe etiquetas de clasificación de datos, aunque los secretos industriales deberían generalmente obtener la clasificación más alta, excepto en ambientes militares y diplomáticos. Una designación de clasificación de datos está separada y es distinta de una designación de secreto industrial. Cada designación implica diferentes acciones para proteger los datos correspondientes. Esta política evita que otros dentro de la organización declaren como secreto industrial a una información que de hecho no puede considerarse tal.

Políticas Relacionadas: “Divulgación de Secretos Industriales” y “Lógica Crítica de Negocios”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

8. Etiquetas Incorrectas de Clasificación de Datos

Política: Si el receptor de la información interna de la Empresa X piensa que es incorrecta la etiqueta de clasificación que tiene la información, debe proteger la información de la manera que corresponda con la más rigurosa de las dos formas posibles de etiquetas de clasificación y confirmar con el Propietario de la Información que la etiqueta ahora colocada a la información es la correcta.

Comentario: La orientación que ofrece esta política a menudo no se encuentra en declaraciones de políticas de clasificación de datos, pero debe añadirse para guiar a los receptores de la información. Esta política requiere que se verifique con el Propietario de la información antes de tomar alguna decisión en el manejo apropiado de la información que tenga una etiqueta sospechosa. Esta política sólo se aplica a la información interna para mantener los costos bajos y restringir el alcance de la política. Existe la posibilidad de expandirla para incluir información suministrada externamente que ahora está en manos de la Empresa X. La decisión hace referencia a la más rigurosa de las dos etiquetas posibles. Si el receptor piensa que la información debe ser "confidencial" pero en realidad sólo está marcada como "sólo para uso interno", entonces el receptor debe tratarla como confidencial hasta que reciba instrucciones del Propietario de la información para hacer lo contrario. De igual manera, si piensa que debe ser etiquetada para uso interno y está etiquetada como confidencial, debe tratarla como tal hasta tener instrucciones en contrario. Este proceso decisivo de la clasificación a veces se denomina "lo alto del sistema", reflejando el hecho de que al combinarse información de varias clasificaciones prevalece la etiqueta de mayor seguridad. Esta política asume que se adoptó un sistema formal de clasificación de datos.

Políticas Relacionadas: "Etiqueta de Sensibilidad Desconocida" y "Etiquetado de Clasificación Múltiple"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

9. Asignación de Etiquetas de Clasificación de Datos

Política: Para todos los tipos de información de producción existentes, el Propietario de la información es responsable de escoger una etiqueta de clasificación de datos apropiada a usar por los trabajadores que reproducen, compilan, alteran o procuran información de producción.

Comentario: Esta política especifica quién debe escoger y aplicar una etiqueta de clasificación de datos, también conocida como marca. La asignación de la responsabilidad que se hace en esta política no es la única opción. Otros grupos que pueden ser designados para tomar decisiones incluyen un gerente del que se origina la información y un tercero que suministra la información.

El objetivo importante aquí es estar claro sobre quién toma la decisión y garantizar que estas mismas personas tengan un adiestramiento adecuado para tomar una decisión justificada. Esta política es apropiada para un laboratorio de investigación y desarrollo u otras organizaciones donde el personal tiene amplitud para tomar sus propias decisiones. Aquellas organizaciones que optan por no darle amplitud a su personal deben insistir en que la clasificación de datos la hagan los Propietarios o los gerentes. Por razones de costos esta política es deliberadamente limitada a la información de producción, pero podría ampliarse para incluir todos los tipos de información definidos en un diccionario corporativo de datos. Cuando varios tipos de información de poca sensibilidad se combinan, pasan a ser de mayor sensibilidad.

Políticas Relacionadas: "Restricciones a la Recopilación de la Información" y "Etiquetado Durante el Ciclo de Vida de la Información"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

10. Etiquetado de Clasificación Múltiple

Política: Cuando información de distintas clasificaciones de sensibilidad se combinan, la información que resulta debe ser clasificada en el nivel más restringido de cualquiera de las fuentes.

Comentario: Esta política orienta a los usuarios en el correcto etiquetado de los archivos, bases de datos, discos flexibles, CD-ROMs, y otras recopilaciones de información. A menudo informaciones con diversos tipos de sensibilidad se combinan y los usuarios no saben qué tipo de etiqueta colocar al producto resultante. Esta política utiliza el concepto militar de "lo alto del sistema" que sostiene que la recopilación de información resultante, debe adoptar los más altos y rigurosos requerimientos encontrados dentro de la información. Esta política asume que ya existe un sistema de clasificación y la noción de clasificaciones de sensibilidad ha sido participada a los usuarios.

Políticas Relacionadas: "Restricciones a la Recopilación de la Información" y "Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

11. Exposición de Medios a Datos Secretos

Política: Cualquier medio de almacenamiento que pueda ser modificado, como los discos flexibles, las cintas magnéticas o los CD-RW y que haya sido expuesto a datos o aplicaciones confidenciales, debe ser clasificado a ese nivel.

Comentario: Esta política indica a los usuarios la forma correcta de asignar etiquetas para medios de almacenamiento luego de que éstos hayan sido expuestos a datos o aplicaciones secretas. En lugar de "secreto" otro término puede ser utilizado. Esta política es necesaria en ambientes de alta seguridad porque los medios de almacenamiento con la capacidad de ser escritos en computadores pueden tener archivos temporales, archivos transitorios y otros archivos de trabajo almacenados en ellos sin que el usuario lo sepa. El sistema no borra estos archivos o sólo suprime el listado del directorio para los archivos, en cuyo caso los datos subyacentes se pueden recuperar del medio de almacenamiento. Esta política hace referencia a la "exposición" a datos o aplicaciones secretas. En este contexto "exposición" simplemente significa que se utilizó en un computador mientras estaban activos datos o aplicaciones secretos. Una aplicación no secreta puede estar trabajando en datos secretos, en cuyo caso algunos de los datos secretos pueden quedar registrados en el medio de almacenamiento del computador. De igual manera, una aplicación secreta puede almacenar información temporal en un computador. Aun cuando las aplicaciones son designadas correctamente, esta política es aplicable ya que puede haber una falla en la electricidad, interrupción por el usuario, error en el sistema operativo o cualquier otro problema que evite que se borre como fue planeado originalmente. Reclasificación a nivel secreto significa que se requieren procesos especiales de eliminación para los medios de almacenamiento.

Políticas Relacionadas: “[Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad](#)” y “[Etiquetado de Clasificación Múltiple](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

12. Etiquetas de Clasificación Generadas por Usuarios

Política: Las etiquetas de clasificación asignadas por otra persona distinta al Propietario de la información designado, no restringe en forma alguna el derecho de la Empresa X a utilizar o acceder a esta información.

Comentario: Esta política notifica a los usuarios que no importa si colocan la palabra "privado" u otra etiqueta en un mensaje de correo electrónico o en el nombre de un archivo del directorio. Este material puede ser accedido por el personal de la Empresa X si por alguna razón lo considera necesario. Esto significa que los usuarios no tienen un dominio privado en el computador cuando utilizan los sistemas informáticos de la Empresa X. Esta política anima a los usuarios a ocuparse de cosas personales en los computadores en casa o en otras instalaciones. Esta política desanima el uso personal de los sistemas informáticos de la Empresa X y, además, establece claramente que sólo el Propietario puede asignar una etiqueta de sensibilidad y que todas las demás etiquetas de sensibilidad pueden ser ignoradas sin ninguna penalización.

Políticas Relacionadas: “[Uso Personal de los Sistemas de Computación y de Comunicaciones](#)” y “[Propiedad de la Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

13. Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad

Política: Si un sistema de computación contiene información con diferentes clasificaciones de sensibilidad, los controles usados deben reflejar la información más sensible residente en el sistema.

Comentario: Esta política garantiza que la información sensible no será divulgada incorrectamente sólo porque está en el mismo sistema con información menos sensible. Aun cuando es un objetivo costoso en el diseño de sistemas, esta política sostiene que la información debe ser protegida de acuerdo a las "más altas" clasificaciones residentes en el sistema. Entre los militares esto es conocido como política de "lo alto del sistema". Los costos relacionados con la seguridad pueden reducirse significativamente si la información más sensible se pasa a otro sistema o segmentando los datos por su sensibilidad a una unidad de disco diferente y a otros componentes del sistema. Varios componentes segmentados del sistema que contienen datos similares clasificados pueden ser accesibles solamente cuando el procesamiento en el sistema se está realizando a cierto nivel de seguridad. Por ejemplo, si un procesamiento confidencial se está realizando en un sistema, entonces los discos secretos son inaccesibles. Esta política indicaría, por ejemplo, que los mecanismos de control de acceso al sistema operativo, deben tener la fuerza suficiente para proteger la información más sensible del

sistema. Esto significa que todos los otros tipos de información deben soportar la carga general de este tipo de información más sensible. Esta política se aplica más rápidamente a un sistema aislado y se vuelve compleja cuando se trata de redes. Llevándolo a su conclusión lógica, todos los sistemas conectados a la red deben tener los mismos tipos de controles, consistentes con los datos más sensibles que han de manejarse.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Exposición de Medios a Datos Secretos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

14. Clasificaciones de Medios de Almacenamiento de Datos

Política: Si la información registrada en un medio de almacenamiento del computador con una clasificación de sensibilidad alta se pasa a otro medio con una clasificación de sensibilidad baja, entonces el medio con la clasificación de sensibilidad baja debe ser actualizado para que su clasificación refleje la clasificación de sensibilidad más alta.

Comentario: Esta política ofrece pautas específicas para usuarios finales y otros que manejen medios de almacenamiento de datos como CD-ROM, discos flexibles, cintas de audio digitales y cintas de nueve pistas. Les dice cómo deben proceder cuando los archivos u otras recopilaciones de datos tienen clasificaciones diferentes de datos. Por ejemplo, si el disco duro tiene información secreta y se escribe información del disco duro en un disco flexible que tiene información confidencial, entonces el disco flexible debe ser reclasificado como secreto. En vez de mezclar información con diferentes clasificaciones, algunas organizaciones escogen utilizar medios diferentes de almacenamiento de datos para cada clasificación; por ejemplo, los discos flexibles de ahora en adelante pueden tener etiquetas de color indicando la clasificación de la información allí almacenada. Se pueden utilizar otros controles para manejar rápidamente las múltiples clasificaciones de datos almacenados en el mismo medio. Por ejemplo, los datos secretos pueden estar cifrados mientras que los datos no clasificados pueden dejarse sin cifrar.

Políticas Relacionadas: “Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad” y “Almacenamiento de Información de Clasificación Mixta”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

15. Fecha de Desclasificación

Política: Si se conoce, la fecha en que la información secreta, confidencial o privada dejará de ser sensible debe indicarse como parte de la información de la clasificación.

Comentario: Esta política garantiza que la información será degradada a una clasificación menor cuando sea necesario. Por ejemplo, si la información sobre una fusión y adquisición es secreta, ésta se convierte en pública desde la fecha en que se anuncia. En vez de una fecha específica, el Propietario puede mencionar un evento particular, como la fusión. Con el tiempo se manifiesta una tendencia natural a clasificar de un nivel más alto la información o, por lo menos, a permanecer sobre-clasificada. Esta política lucha contra estas tendencias y mantiene los costos de seguridad bajos porque se reducen los costos del control de acceso. La fecha de degradación de la clasificación, también conocida como fecha de vencimiento, puede indicar el momento para desechar la información para reducir los costos de almacenamiento. La clara indicación de la fecha de degradación de la clasificación también facilita el manejo ordenado de la información por personas que pueden no estar en comunicación directa con los otros involucrados. Esta política asume la existencia de una política en la cual se definen los términos “secreto, confidencial o privado”.

Políticas Relacionadas: “Retención de la Información Sensible” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

16. Desclasificación Acelerada de la Información

Política: El Propietario de la información puede desclasificar o degradar en cualquier momento la clasificación de sensibilidad que se aplica a la información, mediante el cambio de la etiqueta de clasificación que aparece en el documento original, notificando a todos los receptores conocidos y al Custodio de los archivos de la Empresa X.

Comentario: Esta política aclara lo que tiene que suceder para desclasificar o degradar la clasificación de la información. La desclasificación involucra la remoción de una etiqueta que indica la sensibilidad de la

información, mientras que la degradación involucra mover la información a un nivel inferior de sensibilidad. La política reconoce de manera implícita que no todas las copias de información serán ubicadas y desclasificadas o ubicadas y degradadas. Los problemas introducidos por la ubicación incompleta de los receptores de la información son aceptables porque estos problemas brindarán más, en vez de menos, seguridad. Algunas organizaciones pueden cambiar las palabras "documento original" para hacer una referencia más específica a las versiones computarizadas del original. Esta política debe ser distribuida sólo a los Propietarios de la información o a aquellos con la autoridad para desclasificar o degradar información. En algunos casos, la gerencia querrá que los Propietarios documenten las razones por las que hubo la desclasificación o la degradación que puedan mencionarse en la política. En lugar de "Custodio de archivos", puede utilizar un cargo como gerente de almacén de datos, administrador de diccionario de datos u otro similar. Típicamente se trata de alguien que mantiene el registro de información sobre la información.

Políticas Relacionadas:“Prórroga para la Desclasificación” y “Acceso de Escritura a Información Sensible”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

17. Prórroga para la Desclasificación

Política: El Propietario de la información designado puede en cualquier momento antes de fijar la desclasificación, prorrogar el período en el cual la información debe permanecer en determinado nivel de clasificación, cambiando la fecha de desclasificación o degradación que aparece en el documento original, notificando a todos los receptores, iniciando una búsqueda eficaz a nivel de costo de receptores adicionales y notificando al Custodio de los archivos de la Empresa X.

Comentario:Esta política especifica lo que debe hacerse para prorrogar la fecha de desclasificación o degradación de la información. La ubicación de receptores adicionales es esencial si la información va a ser protegida adecuadamente. Sin la búsqueda, los receptores que no se enteren de la prórroga pueden de buena fe divulgar la información a terceros no autorizados a menos que otra política les exija verificar con el Propietario antes de divulgar la información. Esta búsqueda puede ser costosa y consumir tiempo a menos que se lleve un libro de registro con los receptores. Para evitar la necesidad de prorrogar la fecha de vencimiento,

algunas organizaciones rutinariamente añaden un mes o un tiempo similar a la fecha en que se espera la desclasificación o degradación. Algunas organizaciones cambiarán las palabras "documento original" para hacer referencia más específica a versiones computarizadas del original. Esta política debe ser distribuida sólo al Propietario de la información o a aquéllos con la autoridad para desclasificar o degradar la información. En algunos casos, la gerencia querrá que los Propietarios documenten la razón para la prórroga de la fecha, lo cual también se puede mencionar en la política.

Políticas Relacionadas:“Desclasificación Acelerada de la Información” y “Acceso de Escritura a Información Sensible”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

18. Cronograma de Desclasificación

Política: La clasificación de sensibilidad de todos los documentos de la Empresa X debe ser rutinariamente degradada de acuerdo con la Tabla 3-3 excepto cuando un tipo de documento haya sido eximido o cuando el Propietario de la información haya suministrado instrucciones distintas para la desclasificación o degradación.

Tabla 3-3: Cronograma de Desclasificación

Existente	Nuevo	En X Años
Secreta	Confidencial	10
Confidencial	Sólo Uso Interno	15
Sólo Uso Interno	Pública	20

Comentario:La intención de esta política es obligar a la desclasificación o degradación automática de la información sensible, porque muchos documentos se dejan en su clasificación original durante un tiempo excesivo. Esto significa que los trabajadores tendrán dificultad ubicando y accediendo a información que de otra manera habría estado disponible, lo cual trae como resultado que los costos de seguridad suban más de lo necesario. Otra razón para contar con un proceso de desclasificación y degradación automática es apoyar la discusión abierta de política e historia, y aprender de dicha información sin obstaculizar excesivamente la gestión actual. La desclasificación automática de documentos garantiza que la desclasificación y

degradación se hará aún cuando el Propietario de la información no se ocupe de ello. Un sistema automático de desclasificación también significa que será eliminada parte de la subjetividad que rodea al proceso de desclasificación y degradación. El número de años que pasarán hasta que se dé la degradación automática varía según la organización. De igual manera, algunas organizaciones preferirán nunca hacer pública la información. Esta política asume que la Empresa X utiliza sólo tres niveles de clasificación de datos sin incluir la "pública". Debido a la complejidad del proceso de desclasificación automática, éste se aplica mejor con un sistema de manejo de documentos y otras herramientas computarizadas similares. En otro particular, los documentos exentos no sujetos a la degradación automatizada pueden incluir reportes médicos, archivos de personal, quejas internas y archivos de resolución de disputas, archivos cliente-abogado, e información relacionada. Algunas organizaciones también querrán expandir la política por razones de privacidad para especificar que la información pertinente a una organización externa no debe ser degradada sin el consentimiento previo de dicha organización. Esta política generalmente es distribuida sólo a los Propietarios de la información y a otros que toman decisiones sobre la clasificación de la información.

Políticas Relacionadas: “Fecha de Desclasificación” e “Información Liberada al Público — Autorización”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

19. Revisión Anual de la Desclasificación

Política: Al menos una vez al año los Propietarios deben revisar la clasificación de sensibilidad asignada a la información por la cual son responsables.

Comentario: La información sensible tiende a ser sobre-clasificada con el paso del tiempo. Por ende, son necesarias medidas para desclasificarla o degradarla si queremos mantener los costos de seguridad informática al mínimo. La desclasificación de la información también mantiene la responsabilidad de los gobiernos y corporaciones ante los ciudadanos y accionistas. Esta política formaliza un paso para la desclasificación y degradación de la información, y requiere que los Propietarios participen en el proceso. Típicamente se prepara un reporte que señala el tipo de información y su clasificación para que el Propietario de la información lo revise. Los Propietarios simplemente

marcarán las opciones correspondientes a la información o los documentos que deben desclasificarse, degradarse o permanecer clasificados. La revisión anual puede reemplazarse por una revisión periódica o cualquier otra. La política asume que el término "Propietario" ha sido definido en otra parte. En la mayoría de los casos esta política necesita otra política que defina el término "sensible".

Políticas Relacionadas: “Fecha de Desclasificación” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

20. Desclasificación de la Información Sensible

Política: Desde el punto de vista de la sensibilidad, la información debe ser desclasificada o degradada tan pronto sea práctico.

Comentario: Mantener la información en una clasificación excesivamente sensible también mantiene altos los costos de seguridad informática. Puede además ser utilizada inadecuadamente como mecanismo para evitar que ciertas personas autorizadas vean la información. Cuando esto se hace público, queda mal la gerencia, implicándose que tiene algo que ocultar. Esta política revierte la tendencia de clasificar la información a niveles de exceso con el paso del tiempo. Esta política requiere que el término "sensible" se defina en otra política. La desclasificación es apropiada para información que era crítica y que ahora lo es menos, e información que era valiosa y ya no lo es tanto. La mayoría de las organizaciones no tienen esquemas de clasificación que se enfoquen en el valor o criticidad de la información, pero podría adoptarse el mismo enfoque. Algunas organizaciones preferirán otra forma alternativa de redactar esta política, como por ejemplo, "Los Propietarios de la información son responsables de garantizar que los documentos sean clasificados al nivel más bajo correspondiente a las necesidades de la Empresa X".

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” y “Revisión Anual de la Desclasificación”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

21. Desclasificación de Archivos Secretos

Política: Los archivos secretos de la Empresa X deben ser hechos públicos cuando hayan transcurrido 30 años después de los eventos allí descritos.

Comentario: Esta política ayuda a los historiadores, reporteros, escritores, educadores, estudiantes y otros, en la comprensión de la historia. La política también ayuda en el proceso democrático de los países donde se pueden discutir libremente los sucesos históricos. Esta política sería adoptada sólo por una agencia gubernamental o una agencia de alto perfil sin fines de lucro. Con esta política, después de 30 años la información diplomática o militar que en un tiempo fue considerada secreta, puede hacerse pública. Esta información debe revisarse antes de divulgarla para garantizar que no se revelará información esencial para la seguridad de la nación, o se descubrirán fuentes de información como los espías, ni serán revelados métodos de análisis ni de inteligencia en uso actualmente. El mayor riesgo con una política como ésta es que la información que se divulgue es un desafío para los mitos o la propaganda que la gerencia actual busca perpetuar. No hay nada de especial acerca del período de 30 años que se menciona, ya que podría ser cualquier otro período de tiempo.

Políticas Relacionadas: “Desclasificación Acelerada de la Información” y “Destrucción de Registros de Transacciones”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

22. Información y Software Esenciales

Política: La persona designada como Propietario de la información debe determinar si la información, y el software relacionado con ella que se encuentra bajo su control, es esencial en el sentido de que ambos son necesarios para representar el estatus exacto actual del negocio de la Empresa X, para completar una transacción de negocio o para satisfacer los requerimientos legales o regulatorios.

Comentario: Esta política requiere que el Propietario de la información determine si la información es esencial. La distinción es útil al momento de determinar qué

información necesita ser respaldada, qué información necesita ser almacenada fuera del sitio o en otro sitio alternativo de procesamiento de datos, qué información necesita controles de integridad adicionales como los dígitos de verificación de los números de cuentas, y qué información necesita ser considerada dentro del alcance de un plan de contingencia.

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” “Respaldo de Datos,” y “Clasificación de Recursos Informáticos”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

23. Etiquetas de Entradas en Almacén de Datos

Política: Toda información incluida en el almacén de datos de la Empresa X, debe ir acompañada de información acerca de su origen, su clasificación de sensibilidad, su confiabilidad y la fecha de su más reciente revisión.

Comentario: Esta política establece las reglas básicas para poblar un almacén de datos o cualquier otra base de datos. El acceso al almacén de datos debe contener información con los antecedentes necesarios que permitan a la gerencia determinar la integridad de la información subyacente, hasta dónde esa información es confiable y la relevancia de la información para propósitos específicos de toma de decisiones. Sin estos antecedentes, la gerencia sólo estaría adivinando en cuanto a la integridad, confiabilidad y relevancia de la información. Estos antecedentes también son importantes cuando se realice el post-mortem de un proceso fallido de toma de decisiones. La gerencia puede querer saber qué falló y cuáles datos estuvieron errados. Estos antecedentes de la información también son útiles cuando se investigan fraudes o falsificaciones.

Políticas Relacionadas: “Avisos de Derechos de Autor en Software” y “Atribución de la Información”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5.02.02 Etiquetado y Manejo de la Información

1. Retención de Datos en Grupos de Archivos

Política: Los usuarios deben guardar sus archivos en servidores compartidos en directorios que reflejen cuatro agrupaciones; financieros, recursos humanos, investigación y desarrollo, y otros, teniendo dichas agrupaciones sus requerimientos para el control de acceso y la retención de datos.

Comentario: Esta política obliga a los usuarios a categorizar sus archivos de acuerdo al tipo de archivo utilizado. Una vez realizada la categorización, entran en acción varias actividades de seguridad informática. Por ejemplo, la información de investigación y desarrollo puede ser un secreto industrial, o al menos propiedad intelectual y debe ser guardada celosamente. Estos datos pueden por lo tanto ser automáticamente cifrados cuando se almacenan en un disco duro. Como otro ejemplo, los datos financieros deben ser guardados por cierto período de tiempo porque las leyes locales dictan tal cronograma de retención. Las categorías cambiarán dependiendo de la organización. Las mostradas aquí son sólo ejemplos. La designación efectuada por el usuario de un tipo de información es en un sentido un reemplazo inferior de un esquema de clasificación de datos. Es inferior porque usa categorías amplias que requerirán que muchos tipos de información menos sensible sean protegidos en concordancia con la información más confidencial encontrada en esa misma categoría. Este enfoque puede costar más a la larga, pero puede ser atractivo en el corto plazo porque requiere menos adiestramiento e infraestructura organizacional que un sistema de clasificación de datos.

Políticas Relacionadas: “Retención de los Datos de Transacciones con Aplicaciones” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Low

2. Convenciones en Nombres

Política: Para lograr un control de acceso consistente en todos los tipos de sistemas de computación, los códigos normales para identificadores de usuarios, nombres de programas de producción, nombres de archivos de producción, nombres de sistemas y otras convenciones en nombres deben ser soportadas adecuadamente.

Comentario: Esta política de convenciones en nombres facilita la administración de los sistemas de control de acceso de usuarios para múltiples plataformas, las operaciones de registro y las pistas de auditoría. Esta política es un ejemplo útil para establecer un sistema único de registro. Es también útil para los diseñadores de sistemas que crean sistemas de aplicaciones integradas. Sin tales convenciones, es muy difícil realizar ciertas tareas de seguridad. Ejemplos de estas tareas incluyen rastrear las actividades del usuario en varios sistemas y revocar privilegios para todos los identificadores de usuario relacionados con una persona específica después de que esa persona ha sido cesada. Algunas organizaciones pueden querer cambiar algunas palabras de esta política para reflejar intenciones adicionales.

Políticas Relacionadas: “Información de Contacto del Empleado” y “Convenciones en Nombres de Archivos”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Nombres de los Sistemas de Computación

Política: La función que realiza el computador o el software que éste ejecuta no debe ser utilizada en ninguna parte del nombre del computador, si ese nombre es visible desde la red interna de la Empresa X u ocurre en cualquier archivo legible por computador.

Comentario: Esta política dificulta la vida de los hackers, espías industriales, antiguos empleados que buscan venganza y de otros con motivos menos ejemplarizantes. Estas personas pueden forzar la entrada en los sistemas o redes de la Empresa X y empezar a buscar, tratando de adivinar qué van a hacer luego. Si los servidores u otras máquinas son denominados de una manera útil, entonces estos intrusos reciben una ayuda significativa. Por ejemplo, revelando un nombre como “SERVIDOR DE PAGO” informará a los intrusos sobre dónde deben concentrar sus esfuerzos. Por otra parte, si los nombres de los computadores no se relacionan, por ejemplo, los nombres de los planetas en el sistema solar, entonces los intrusos no reciben ayuda con esta información. Puede que a los administradores de sistemas les parezca que esta política dificulta un poco más su trabajo pero, como ellos conocen los nombres de las máquinas con las que trabajan, esto no debería ser un problema grave. Así como la información acerca del sistema alcanzado no debe ser divulgada a los usuarios

antes de estar registrados correctamente, igualmente el nombre del sistema que ellos han alcanzado no debería revelar esta información.

Políticas Relacionadas: “[Señalización de Centros de Computación y Comunicaciones](#)” y “[Convenciones en Nombres de Archivos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Convenciones en Nombres de Archivos

Política: Debe utilizarse una convención para nombrar los archivos de tal manera de distinguir entre aquellos archivos usados para la producción y aquellos archivos usados con fines de prueba y adiestramiento.

Comentario: Una convención para nombrar archivos, que distinga los archivos de producción de otros archivos, ayuda en los respaldos, en los análisis de los registros, en el diagnóstico de problemas y en la administración del sistema. Dicha convención también presta ayuda en la depuración de archivos de prueba y adiestramiento de una nueva aplicación, después de terminados ambos. Esta política permite el manejo automático de los archivos basados en un nombre de archivo. Por ejemplo, un programa de respaldos en la red de área local puede recibir instrucciones en el sentido de sólo respaldar aquellos archivos en cada computador personal que tengan el sufijo ".dat.". Sin estas convenciones los procesos en comandos, tales como la búsqueda de las cintas de respaldo de ciertos archivos, son más difíciles. Convenciones en nombres de archivos como ésta son importantes en ambientes cliente-servidor y de comunicaciones en Internet donde funcionan diferentes sistemas operacionales. Estas convenciones en nombres de archivos son muy útiles si se usa réplicas de datos a lo largo de múltiples máquinas.

Políticas Relacionadas: “[Convenciones en Nombres](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Transacciones Distintas a Producción

Política: Toda transacción utilizada para auditar, probar, adiestrar u otro fin que no sea de producción, deberá estar etiquetada o de alguna manera separada de las transacciones utilizadas para el procesamiento de producción.

Comentario: Esta política claramente separa las auditorías, las pruebas, los adiestramientos y las transacciones no relacionadas a producción, de las transacciones propias del negocio. Si esta separación se logra, se evita tanto la confusión como las actualizaciones inadecuadas de los registros computarizados. El uso de la técnica de auditoría de tecnología informática conocida como "mesa de pruebas" (test deck) involucra, por ejemplo, la presentación de transacciones ficticias al sistema para determinar si las maneja correctamente. Los análisis del mesón de simulacros determinan si los controles están funcionando adecuadamente y si las transacciones fueron colocadas en las cuentas correctas. Una manera de etiquetar estas transacciones es mediante un número serial especial para transacciones, tal vez formado por letras en lugar de números. En otras palabras, no es necesario utilizar un campo especial dedicado exclusivamente a la designación de la producción. Esta información podría ser incorporada a otros campos.

Políticas Relacionadas: “[Transacciones de Entrada en Producción](#),” y “[Capacidad de Reconstrucción de Cambios en Producción](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Divulgación de Secretos Industriales

Política: Los trabajadores deben proteger diligentemente toda la información de la Empresa X específicamente identificada como secreto industrial para que no sea divulgada sin autorización. Los secretos industriales deben ser identificados como tales antes de divulgarse a cualquier trabajador.

Comentario: Esta política comunica a los trabajadores que la Empresa X tiene cierto tipo de información que considera secreto industrial y que espera que los trabajadores protejan dicha información. Desde el punto de vista legal, la política pretende garantizar que los trabajadores que entran en contacto con información altamente sensible sepan que esa información es considerada secreto industrial. Debido a que la mayoría de las organizaciones no cuentan con una categoría aparte en su sistema de clasificación de datos para los secretos industriales, la política define dónde corresponden los secretos industriales con respecto al sistema de clasificación de datos. Algunas organizaciones van un paso más allá al requerir de todos los empleados nuevos, la firma de un acuerdo de confidencialidad que especifica los tipos de información considerados secretos industriales. Esta política va

dirigida a quienes trabajan como empleados, consultores y contratistas ya que se requieren arreglos diferentes para los socios estratégicos de negocios y otros terceros.

Políticas Relacionadas: “Divulgación de Secretos Industriales por Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

7. Etiquetado de Clasificación de Datos

Política: Toda información secreta, confidencial y privada debe estar etiquetada de acuerdo con las normas emitidas por el departamento de Seguridad Informática, mientras que la información que no corresponda a ninguna de estas categorías no necesita etiquetarse.

Comentario: Esta política establece cuáles tipos de información requieren una etiqueta de sensibilidad. Una etiqueta es simplemente una o varias palabras que indican la relativa confidencialidad de los datos. "Secreto", "en confidencia" y "sólo para uso interno" son etiquetas típicas. Se requieren especificaciones separadas acerca de cómo etiquetar, aunque esta información puede ser suministrada en documentos de procedimiento o normas. Por ejemplo, dónde colocar una etiqueta en un computador, en un disco flexible, en un disco duro y otros lugares puede ser especificado en una norma relacionada. El movimiento de la información de un sistema operativo a otro puede ser problemático porque la etiqueta de confidencialidad puede ser arrancada junto con la información de formateo y la relativa a sistemas operativos. Una organización puede desear adoptar normas para presentar las etiquetas de confidencialidad dentro de los archivos, por ejemplo, en la primera línea de los archivos de texto. Esta política supone la existencia de otra política que define los términos "secreto, confidencial y privado". Estos términos pueden ser reemplazados con las etiquetas utilizadas dentro de la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Etiquetado Completo de la Clasificación”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

8. Etiqueta de Sensibilidad Desconocida

Política: Si no se puede determinar una etiqueta de sensibilidad para la información obtenida en instalaciones de la Empresa X que usualmente contienen información secreta, entonces dicha información debe ser tratada como secreta.

Comentario: Esta política especifica cómo manejar información con etiquetas de clasificación de datos desconocidos o no especificados. Esta política suministra un enfoque altamente seguro para tratar con una etiqueta ambigua de clasificación de datos. La mayoría de los sistemas de clasificación de datos utilizan "sólo para uso interno" de manera predeterminada, o un nivel relativamente bajo de sensibilidad. Esta política, en cambio, de manera predeterminada exige la categoría más alta en el esquema de clasificación de datos. Sin esta política, si un trabajador remueve u oscurece una etiqueta secreta, entonces automáticamente la información se desclasifica al estatus de "sólo para uso interno" y esto resulta en la divulgación a personas que no deben tener acceso a esta información. Esta política impone costos adicionales asociados con el manejo de información sin clasificación conocida, pero reduce la cantidad de divulgaciones que se hacen por error. Esta política es apropiada para laboratorios de investigación, unidades militares, una agencia diplomática gubernamental o alguna organización similar de alta seguridad.

Políticas Relacionadas: “Etiquetado de Clasificación de Datos” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

9. Etiquetas de Clasificación por Departamento

Política: Las etiquetas de clasificación de datos específicas por departamento deben ser consistentes con el sistema de clasificación de datos de la Empresa X y complementarlo.

Comentario: Esta política intenta aclarar las circunstancias bajo las cuales es permisible emplear etiquetas departamentales de clasificación de datos. Por ejemplo, en los hospitales debe haber una etiqueta para toda la organización que indique que la información es "privada". Pero dentro del departamento de Archivo, deben ser necesarias etiquetas adicionales como "privado—psicológico" o "privado—financiero". Esta política intenta evitar en los departamentos conflictos o términos confusos que interfieran con el manejo

apropiado de la información. En este caso, si el departamento de Archivos designa historiales privados como "confidencial—psicológico" y "confidencial—financiero", esto sería un problema y una violación de la política. Lo ideal es que no haya etiquetas adicionales necesarias, y que todos los trabajadores a lo largo de la organización utilicen las mismas etiquetas para la clasificación de los datos.

Políticas Relacionadas:“[Identificación de Registros Vitales](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

10. Etiquetado de Información Externa

Política: Con excepción de la correspondencia general de negocios y el software con derechos de autor, toda información suministrada externamente y que no sea del dominio público, debe ser asignada una etiqueta con la clasificación de datos de la Empresa X por la persona que la recibe.

Comentario:Esta política especifica quien debe etiquetar la información suministrada externamente que no es del dominio público. Esta política va más allá, especificando que las etiquetas suministradas por el tercero externo no deben ser modificadas o borradas. Esta política también puede especificar que el receptor de la Empresa X es el Propietario inicial de la información y que con el tiempo el papel de Propietario de la información puede pasar a otra persona. Esta política intenta aclarar un área llena de confusión y ambigüedades, porque en muchos casos la información sensible suministrada externamente no es protegida adecuadamente por la organización receptora, ya que la responsabilidad de asignar la etiqueta del sistema de clasificación de datos no ha sido claramente especificada. Esto significa que personas que entran en contacto con la información, pueden no manejarla adecuadamente.

Políticas Relacionadas:“[Asignación de Etiquetas de Clasificación de Datos](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Medianos y altos

11. Etiquetas de Clasificación Para Nueva Información

Política: Todo usuario que produzca archivos de computador o mensajes debe seleccionar una de las etiquetas de clasificación de datos autorizada al momento de guardar o enviar dichos archivos y mensajes.

Comentario:Esta política coloca etiquetas de clasificación de datos en archivos y mensajes nuevos desde el momento en que fueron creados, y mantiene estas mismas etiquetas fijadas a la información correspondiente a lo largo del ciclo de vida de la información o hasta que la clasificación se cambie. Si una etiqueta es fijada al momento de crear la información, lo más probable es que siga a la información a medida que ésta cambia de forma y ubicación. Por ejemplo, si un mensaje de correo electrónico se etiqueta como confidencial cuando se prepara, cuando el receptor vea esta información estará alerta al hecho de que es confidencial. Cuando este mismo receptor habla por teléfono sobre la información, la etiqueta puede y debe propagarse con la información. Esta política es consistente con la noción de que la información debe ser protegida de acuerdo a su confidencialidad, criticidad y valor, sin importar qué tecnología se usa para procesarla, qué forma adquiere, quién entra en contacto con ella y dónde es enviada. Esta política es inconsistente con otra política de clasificación de datos en la cual los Propietarios de la información tienen la responsabilidad de asignar la etiqueta de clasificación apropiada. Esta política asume la posición de que en toda la organización continuamente se crea nueva información y estos creadores no tienen el tiempo ni la inclinación para estar repetidamente acudiendo a los Propietarios de la información para obtener la clasificación apropiada. Es por ello que algunos paquetes de software instan al usuario a asignar una clasificación al momento de crear un archivo o mensaje nuevo.

Políticas Relacionadas:“[Etiquetado Completo de la Clasificación](#)” y “[Etiqueta de Sensibilidad Desconocida](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Medianos y altos

12. Etiquetado Completo de la Clasificación

Política: Todos los discos, cintas y otros medios de almacenamiento de computación que contengan información secreta, confidencial o privada deben ser etiquetados externamente con la clasificación de sensibilidad apropiada.

Comentario: Esta política suministra lineamientos a todos los trabajadores sobre la necesidad de las etiquetas de sensibilidad, las cuales se requieren todo el tiempo. Esta política sería usada por organizaciones preocupadas por el manejo de la información sensible, mientras que otras la considerarán difícil y demasiado costosa. Antes de utilizar esta política, la gerencia debe determinar que los costos adicionales asociados con el etiquetado completo se justifican dado el riesgo que se corre cuando la información no se etiqueta. Esta política supone la existencia de una política que define los términos "secreto, confidencial y privado". Estos términos pueden fácilmente cambiarse por las etiquetas que se utilizan dentro de la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Etiquetado de Clasificación de Datos”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

13. Etiquetas de Sensibilidad en Papel

Política: Todas las manifestaciones legibles por humanos, impresas o escritas a mano de información secreta, confidencial o privada deben tener una etiqueta de sensibilidad apropiada en la esquina superior derecha de cada página.

Comentario: Esta política suministra la pauta de la ubicación apropiada de las etiquetas de sensibilidad. Algunas organizaciones pueden añadir palabras acerca de la ubicación de las etiquetas de sensibilidad en las etiquetas de los discos flexibles y otros medios de almacenamiento, en cuyos casos el alcance y el título de la política se deben cambiar. Las dos últimas palabras de la política requieren una etiqueta en cada página. Esto evita que se divulgue por error información sensible cuando es copiada o extraída de un documento más largo. Algunas organizaciones son menos restrictivas, requiriendo una etiqueta de sensibilidad en cada página sólo para los tipos de información más sensibles. Esta política supone la existencia de una política que define los términos "secreto, confidencial y privado". Estos términos pueden ser cambiados por los que utiliza la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

14. Etiquetado de Material Impreso Encuadrernado

Política: Si está encuadrernada, toda información secreta, confidencial o privada impresa, escrita a mano y en cualquier otra manifestación tangible, debe tener la etiqueta de sensibilidad apropiada en la cubierta, en la página de título y en la cubierta posterior.

Comentario: Esta política suministra pautas específicas para la colocación apropiada de las etiquetas de clasificación de datos relacionadas a su sensibilidad. Se requiere una etiqueta en la página de título y en las cubiertas anterior y posterior, puesto que la portada puede dañarse o perderse. Algunas organizaciones establecen que se necesita una etiqueta en cada página, pero esto sólo se hace con la información más sensible. Esta política puede modificarse para reflejar las normas existentes en la organización referentes al manejo de sus impresos de manera segura. Esta política presume la existencia de una política que define los términos "secreto, confidencial y privado". Estos términos se pueden reemplazar con las etiquetas utilizadas dentro de la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Etiquetado de Productos y Servicios Peligrosos”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

15. Presentación de la Información Sensible

Política: Si la información es secreta, confidencial o privada, todas las formas en las cuales se despliega en una pantalla o es presentada al usuario deben indicar la sensibilidad de la información.

Comentario: Esta política suministra lineamientos a los desarrolladores de sistemas para desplegar las etiquetas de clasificación de datos sensibles. Esta política puede acompañarse de diagramas y ejemplos que muestren las palabras exactas de cómo va a visualizarse y la exacta ubicación en la pantalla. En algunas organizaciones estos ejemplos incluyen información adicional, tales como las instrucciones para descargar o copiar datos sensibles. Esta política supone la existencia de una

política que define los términos "secreto, confidencial y privado". Estos términos pueden ser reemplazados con las etiquetas utilizadas dentro de la organización.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#),” “[Etiquetado Completo de la Clasificación](#),” “[Cubrir Información Sensible](#),” “[Visualización e Impresión de Contraseñas](#),” y “[Avisos de Derechos de Autor en Software](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

16. Etiquetado Durante el Ciclo de Vida de la Información

Política: Desde el momento en que la información se crea hasta que se destruye, debe estar etiquetada en cuanto a su grado de sensibilidad, ya sea designada secreta, confidencial o privada.

Comentario: Esta política indica que deben fijarse etiquetas a la información sensible vaya donde vaya, cualquiera sea la forma que adopte, sea quien sea que la maneje y con cualquier tecnología que se utilice para procesarla. Si la información contenida en un servidor departamental se descarga a un computador personal, la etiqueta de confidencialidad debe ir adjunta. De igual manera, los controles de acceso deben ser consistentes con los cambios de forma, ubicación y presentación de la información. La ausencia de las etiquetas apropiadas muchas veces evita que la información se maneje en la forma adecuada. Si una información "secreta" no está clasificada porque no está etiquetada, no será manejada con la seguridad necesaria. La remoción de la etiqueta es entonces un medio eficaz para desclasificar y obtener acceso a información sensible. Esta política supone la existencia de una política que define los términos "secreta, confidencial y privada". Estos términos pueden ser reemplazados con las etiquetas utilizadas dentro de la organización.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Etiquetado Completo de la Clasificación](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

17. Mantenimiento de Etiquetas de Clasificación

Política: Los trabajadores que se encuentren en posesión de cualquier información que contenga etiquetas de sensibilidad de la clasificación de datos de la Empresa X, deben mantener, propagar y, de ser necesario, restablecer dicha etiqueta cada vez que la información cambie su forma, el formato o la tecnología con la que se maneja.

Comentario: Esta política informa a los usuarios que deben ser diligentes al cambiar la forma, el formato o la tecnología con la que se maneja la información sensible. Por ejemplo, supóngase que la información etiquetada como "confidencial" se envió por fax a una ubicación remota, y el receptor extrae ciertos detalles del fax y los incluye en un mensaje de correo electrónico. Esta política requiere que la etiqueta "confidencial" se incluya en este mensaje de correo electrónico. Debido a que los usuarios están en control de muchos de los cambios que ocurren en cuanto a forma, formato y tecnología de manejo de la información, ellos son los que deben garantizar que continúe fijada la etiqueta sobre la información sensible. Esta política puede expandirse para incluir etiquetas y restricciones suministradas por terceros, tales como los derechos de autor.

Políticas Relacionadas: “[Etiquetado de Clasificación de Datos](#)” y “[Etiquetas de Clasificación Para Nueva Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

18. Copiado de Información Sensible

Política: No deben hacerse copias adicionales o imprimirse copias extras de información secreta, confidencial y privada, sin la autorización del Propietario de la Información.

Comentario: La intención de esta política estricta es notificar a todos aquellos que entran en contacto con información sensible, que va en contra de la política hacer copias no autorizadas. Otra manera de hacer esto sería involucrar al Propietario de la Información como el único que puede hacer copias de material sensible. Sin embargo, el Propietario puede delegar esta actividad, y en la mayoría de los casos lo hace. Una manera eficaz de implementar esta política es no hacer copias en papel con información confidencial en una máquina copiadora común y corriente. Por lo general, son de color azul u otro color distinto del blanco. Esta

política es importante en aquellos casos en los cuales el material sensible debe ser llevado en registro. Esta política asume la existencia de una política que define los términos "secreta, confidencial y privada". Estos términos pueden ser reemplazados con las etiquetas usadas dentro de la organización.

Políticas Relacionadas: "Prevención del Copiado de Documentos Sensibles," "Registro del Movimiento de Documentos Secretos," "Clasificación de Datos en Cuatro Categorías," y "Seguimiento de Información Sensible"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

19. Seguimiento de Información Sensible

Política: Cada vez que se obtengan copias adicionales de información sensible, se debe anotar en un registro el número de copias y los nombres de los receptores de dichas copias, y cada uno de los receptores debe ser informado que podrá distribuir o hacer copias adicionales sólo después de obtener el permiso del Propietario de la información.

Comentario: Esta política garantiza el seguimiento de todas las copias de la información confidencial, ayudando esto en las investigaciones sobre filtraciones o divulgaciones no autorizadas. Llevar constancia de esto también fomenta un comportamiento responsable al momento de hacer pública la información sensible a terceros no autorizados, hacer más copias o al destruir la información. El registro mencionado en la política debe ser llevado por el Propietario o por una persona que el Propietario designe como punto autorizado de distribución. La referencia al registro es deliberadamente ambigua puesto que puede implantarse de varias maneras. Por ejemplo, la dirección completa de cada receptor puede ser parte del documento en sí mismo, o cada copia puede ser numerada y llevarse constancias separadas de los receptores. En muchos casos las palabras "información sensible" pueden ser reemplazadas por las palabras "información secreta" u otro indicador del tipo de información más sensible en uso en la organización.

Políticas Relacionadas: "Copiado de Información Sensible" y "Registro del Movimiento de Documentos Secretos"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

20. Productos Intermedios Con Información Sensible

Política: Si una máquina copiadora se tranca o funciona mal cuando los trabajadores están haciendo copias de información secreta, éstos no deben abandonar las máquinas hasta que todas las copias de la información sean removidas de la máquina o destruidas por completo.

Comentario: Esta política garantiza la no divulgación de partes y pedazos de información sensible de manera inconsciente, debido a un mal funcionamiento de la maquinaria o algún problema parecido. Esto puede ocurrir cuando el papel que contiene información sensible se deja en una máquina copiadora trabada y luego llega a personas no autorizadas. Aunque la política menciona máquinas copiadoras, puede extenderse para incluir impresoras, máquinas de fax y otras máquinas que manejen información sensible. El alcance de esta política debe restringirse al manejo de información muy sensible relativa a controles internos, tales como las claves de cifrado. Se supone la existencia de una política que define el término "secreta". Este término puede ser reemplazado con la etiqueta que se utiliza en la organización. Una política relacionada requiere que una persona autorizada esté presente cada vez que información sensible vaya a ser transmitida en una máquina de fax o impresa en una impresora.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías," "Envío de Información Sensible Vía Fax — Notificación," e "Impresión de Información Sensible"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

21. Copias Sobrantes de Información Sensible

Política: Todas las copias sobrantes de información secreta que se generen en el curso de copiado, impresión y cualquier otro manejo, deben ser destruidas de acuerdo con los procedimientos autorizados.

Comentario: Esta política notifica a los empleados que cualquier producto intermedio de su trabajo, en este caso copias o impresiones no aceptables, debe ser destruido de acuerdo con los procedimientos autorizados. A menos que se notifique lo contrario, algunos trabajadores simplemente pueden colocar estas copias en un cesto de reciclaje. Esta política puede ser restringida para que sólo se aplique al manejo de información confidencial relacionada con los controles internos, como el manejo de las claves de cifrado. Esta

política supone la existencia de una política que define el término "secreto". Este término puede ser reemplazado con la etiqueta que se utiliza dentro de la organización. Una política relacionada requiere la presencia de una persona autorizada cada vez que información sensible esté siendo transmitida vía fax o impresa en una impresora.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Envío de Información Sensible Vía Fax — Notificación,” e “Impresión de Información Sensible”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

22. Impresión de Información Sensible

Política: Las impresoras deben estar atendidas por personal autorizado para examinar la información que se está imprimiendo o que pronto se imprimirá en el caso de información sensible, a menos que se utilicen controles físicos de acceso para evitar que personas no autorizadas entren al área de la impresora y visualicen el material que se está imprimiendo.

Comentario: Esta política garantiza que ninguna persona no autorizada examinará materiales impresos sensibles. Esto es de particular interés cuando las impresoras son utilizadas por muchas personas, o cuando la impresora se encuentra en un lugar distante de la persona que originó la impresión. A pesar de que la política principalmente está dirigida para el uso en redes de área local, también es aplicable en otros ambientes computarizados, incluyendo servidores departamentales, mainframes, centros de impresión comerciales y operaciones manufactureras. Algunas organizaciones querrán aumentar esta política con palabras que requieran que la persona que está originando la impresión sea la responsable del manejo correcto del material impreso. Esta política puede redactarse nuevamente para reemplazar la palabra "sensible" con la etiqueta específica de clasificación de datos que se utiliza dentro de la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Envío de Información Sensible Vía Fax — Notificación”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

23. Responsabilidad por la Información Sensible

Política: Toda información sensible de la Empresa X impresa en papel debe indicar tanto la página actual como la última en cada página del documento, tal como "Página X de Y".

Comentario: Esta política garantiza que no se perderá ninguna parte de la información confidencial y que los lectores de esta información sabrán que han leído todo el documento. Este procedimiento también ayuda a aquéllos que trabajan en un centro de copiado o de impresión a responsabilizarse por todas las páginas. Esta política no es necesaria para tipos de información menos sensibles porque la responsabilidad por versiones de información menos sensible en formatos impresos tiene menos interés para la gerencia y quizás no vale la pena. Esta es una política de integridad de la información ya que garantiza que toda la información está completa. La política aquí descrita puede ser redactada para que la palabra "sensible" se cambie por la etiqueta específica de clasificación de datos que se utiliza dentro de la organización.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Seguimiento de Información Sensible”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

24. Prevención del Copiado de Documentos Sensibles

Política: Cuando se deba suministrar copias impresas de información privada, confidencial o secreta de la Empresa X a terceros, dichas copias deben ser distribuidas exclusivamente en un papel especial que no permita copias en una fotocopiadora regular.

Comentario: Esta política evita que los receptores hagan copias no autorizadas que generen la diseminación secundaria no autorizada de la información. Este tipo de diseminación secundaria involucra una emisión sin control de la información a personas desconocidas. Por ejemplo, en las etapas iniciales de un juicio, la contraparte puede utilizar procedimientos de descubrimiento para obtener acceso a cierta información sensible interna. El uso del papel especial, que no puede ser copiado, ayuda pero no garantiza que estos terceros tendrán una sola copia de la información, la cual puede ser devuelta posteriormente al Propietario de la información. El uso de papel especial garantiza que la copia devuelta es la copia originalmente distribuida. No

hay nada que evite que los terceros lean la información y luego la descarguen en un computador, le tomen fotos o de alguna manera hagan otra versión del material original que sí puede copiarse. Esta política, sin embargo, sí evita el uso de la tecnología de reconocimiento de caracteres, no sólo la de la tecnología del fotocopiado. Esta política tiene la intención de hacer considerablemente más difícil que las personas no autorizadas hagan copias. Teniendo las alternativas de presentar copias en discos flexibles, CD-ROM o en papel, algunas organizaciones prefieren hacer la distribución en papel como éste ya que es muy fácil hacer copias no autorizadas con otros medios de almacenamiento de datos. La política puede ser ampliada para ser aplicada a todas las copias impresas que contengan información sensible, sin importar que se distribuyan copias a terceros. La desventaja de la amplia aplicación de esta política es que el papel es algo difícil de leer, ya que tiene un fondo de color. La referencia a "Propietario de la información" puede ser cambiada para referirse a la gerencia de Seguridad Informática, gerencia de Seguridad Industrial o al jefe principal de Información. Esta política da mejores resultados cuando se acompaña de otra política que requiera el seguimiento de todas las copias que contengan información sensible.

Políticas Relacionadas: "Seguimiento de Información Sensible" y "Medios de Almacenamiento de Archivos"

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

25. Impresión de Información Secreta

Política: La información secreta de la Empresa X puede ser impresa solamente en papel que muestre claramente que es un original o una copia mediante el uso de bordes coloreados, marcas de agua, u otra tecnología aprobada para su uso por el departamento de Seguridad Informática.

Comentario: Esta política mantiene toda la información secreta impresa en un papel especial que indica que es un original autorizado. El copiar información secreta está prohibido excepto cuando se hace con la autorización del Propietario. La distribución debe ser celosamente seguida a través de registros y otros mecanismos como acuses de recibo. Debido a que sólo el Propietario o un delegado deben tener una versión computarizada de la información secreta, estas personas autorizadas serán las únicas que pueden generar una copia en papel especial. Todos los demás, aún teniendo acceso al original en papel sólo podrán hacer copias en

papel. Este control limita la distribución no autorizada de información secreta a los canales aprobados. Cualquier persona que obtenga una copia en papel de información secreta sabrá si es una copia no autorizada y, si lo es, quien la reciba debe reportar la situación al Propietario. Palabras al respecto pueden incluirse en el documento. La tecnología utilizada para apoyar esta política es básicamente la misma usada para evitar copias de billetes, cheques de viajeros y cheques normales. Como un punto aparte, se debe tener a mano un inventario suficiente de este papel especial si se quiere que esta política sea práctica, y el acceso a los depósitos de los papeles especiales debe estar restringido con controles físicos de acceso.

Políticas Relacionadas: "Registro del Movimiento de Documentos Secretos" y "Prevención del Copiado de Documentos Sensibles"

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

26. Entrega de Salidas Computarizadas Confidenciales

Política: Todo trabajo producido por el computador, bien sea privado, confidencial o secreto debe ser entregado personalmente a los destinatarios designados y nunca debe ser dejado desatendido en un escritorio, o dejado al descubierto en una oficina vacía.

Comentario: Esta política instruye específicamente a los trabajadores en el sentido de no dejar información sensible generada por un computador en lugares donde personas no autorizadas podrían examinarla o robarla. Esto es muy importante en ambientes donde hay mucha gente que tiene acceso a las salidas generadas por computadores como las que salen de impresoras conectadas a un mainframe. La política no prohíbe a operadores de computadores, personal de control de datos y otras personas en posiciones de confianza manejar este tipo de producto computarizado en el transcurso de sus actividades. El manejo especial que requiere esta política para la información sensible recae en la existencia de etiquetas apropiadas impresas en el computador generador de la salida. La política aquí descrita supone la existencia de una política que define los términos "privado, confidencial, y secreta".

Políticas Relacionadas: "Etiquetado Durante el Ciclo de Vida de la Información" y "Clasificación de Datos en Cuatro Categorías"

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

27. Uso de Mensajeros

Política: Toda información privada, confidencial o secreta impresa que se envíe a través de mensajeros comerciales debe recibir seguimiento a través de un número de guía y debe estar marcada con las instrucciones "se requiere la firma del destinatario".

Comentario: Esta política reconoce la realidad de los negocios y el hecho de que hay que depender de despachadores o mensajeros externos. Conociendo la frecuencia con que son utilizados estos mensajeros, esta política especifica la manera de enviar el material sensible. El número de guía permite al remitente saber dónde está el paquete, si fue recibido y quién lo recibió. La instrucción del requerimiento de firma quiere decir que no se entregará si no lo firma una persona autorizada. En otras palabras, no se dejará en un buzón de correos o en la puerta, de donde podría ser robado. Algunas organizaciones van más allá con el requisito de la firma, insistiendo en que sólo la persona designada en la dirección es quien puede firmar. Esta política no incluye medios de almacenamiento, como discos flexibles enviados por correo, porque pueden ser cifrados, reduciendo así considerablemente el riesgo de una divulgación no autorizada. Esta política no hace mención de cómo etiquetar información sensible dentro del sobre del mensajero.

Políticas Relacionadas:“[Etiquetado Completo de la Clasificación](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

28. Entrega de Información Secreta

Política: Todas las entregas de información secreta deben ser conducidas de tal manera que el receptor acuse recibo formal de la información recibida.

Comentario: Esta política garantiza que la información secreta ha sido entregada al receptor designado. Este proceso es a veces llamado "acuse positivo de recibo". El receptor puede llamar al remitente, enviar un correo electrónico o firmar una declaración. En ambientes estrictos de alta seguridad, el receptor debe firmar algo antes de recibirla. Un método específico para acusar recibo podría ser incorporado a la política, a pesar que

esto disminuye su aplicabilidad general. La política también tiene la intención de evitar que personas subsecuentemente nieguen el recibo de la información, y por consiguiente no hacerse responsables del destino de la información. También podrían mencionarse en esta política los requerimientos específicos de tiempo para el acuse de recibo. Esta política asume la existencia de una política que define el término "secreto". Este término puede ser remplazado con la etiqueta utilizada dentro la organización.

Políticas Relacionadas:“[Registro del Movimiento de Documentos Secretos](#),” “[Clasificación de Datos en Cuatro Categorías](#),” “[Recepción de Información Secreta](#),” y “[Recepción de Información de Terceros](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

29. Recepción de Información Secreta

Política: Los receptores de información secreta de la Empresa X deben suministrar por escrito un acuse de recibo formal al momento de tomar posesión de la información.

Comentario: Esta política garantiza que la información secreta será entregada al receptor designado y que el movimiento de dicha información será celosamente seguido con registros actualizados. Un ejemplo común de esta política en acción es la entrega de una citación legal. La entrega sólo puede ser efectuada a la persona nombrada en el documento. El acuse de recibo por escrito es especialmente importante como mecanismo para evitar que los receptores después nieguen haberlo recibido y nieguen la responsabilidad por la información correspondiente. El envío de información sensible a través de intermediarios es aceptable siempre que esté cifrada o sea inaccesible. Esta política es más apropiada y puede ser limitada a fotos, copias impresas y a información legible en otras formas. La política supone la existencia de una política que define el término "secreto". Este término puede ser cambiado por la etiqueta que se utiliza dentro de la organización.

Políticas Relacionadas:“[Registro del Movimiento de Documentos Secretos](#),” “[Clasificación de Datos en Cuatro Categorías](#),” y “[Entrega de Información Secreta](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

30. Registro del Movimiento de Documentos Secretos

Política: Cuando se trate de información secreta, debe mantenerse un registro mientras dicha información retenga la clasificación de sensibilidad secreta, donde se refleje el número de copias hechas, la ubicación de las copias, los nombres de los receptores y cualquier persona que revise las copias.

Comentario: Esta política exige que se mantenga un registro para los documentos más sensibles. Dicho registro puede ser decisivo para determinar si todas las copias han sido recuperadas o destruidas. La existencia del listado tiene un efecto disuasivo, pues recuerda a los posibles transgresores de la política que sus acciones están siendo monitoreadas. La política puede ser ampliada para requerir que todas las copias estén numeradas secuencialmente, aunque no es necesario. Esta política está dirigida a documentos impresos, pero puede ser ampliada para que sea aplicable a la definición de "documento", o a un archivo que pueda incluir audio, formatos, ejecutables y otros tipos de información.

Políticas Relacionadas: ["Clasificación de Datos en Cuatro Categorías,"](#) ["Copiado de Información Sensible,"](#) ["Recepción de Información Secreta,"](#) ["Entrega de Información Secreta,"](#) ["Números Secuenciales para Documentos Secretos,"](#) y ["Seguimiento de Información Sensible"](#)

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

31. Números Secuenciales para Documentos Secretos

Política: Todas las copias de documentos secretos deben ser numeradas de forma individual y secuencial para asegurar que las personas responsables de los documentos y la ubicación de los documentos puedan ser fácilmente encontrados.

Comentario: Esta política garantiza que todos los documentos secretos podrán ser localizados en cualquier momento. Mediante el requisito de la numeración secuencial, todos los documentos secretos se reflejan en un registro o se describen en un reporte. Si aparecen dos copias con un mismo número, entonces se han hecho copias no autorizadas. Cuando esto ocurre, se puede identificar la persona que ha debido evitar la copia. Utilizando la secuencia de números para el rastreo, se dificulta el fraude con documentos secretos. Si la

información secreta cae en manos equívocas, el número de la secuencia indica a quién pertenece la copia que no se protegió adecuadamente.

Políticas Relacionadas: ["Registro del Movimiento de Documentos Secretos"](#)

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

32. Aseguramiento de la Información Sensible

Política: Los trabajadores que tengan la custodia de información sensible, tal como la información confidencial o secreta de la Empresa X, deben tomar las medidas adecuadas para garantizar que este material no esté disponible para personas no autorizadas.

Comentario: Esta política indica que aquéllos que poseen la custodia de material sensible tienen el deber de restringir el acceso a dichos materiales. Materiales sin etiquetas son normalmente definidos, de manera predeterminada, como "sólo para uso interno". El personal interno no necesita restricciones de acceso a este material. La existencia de una etiqueta de clasificación se utiliza para indicar los casos donde la información es sensible. Como otro punto, la política es deliberadamente ambigua acerca de las maneras de restringir el acceso porque variarán de acuerdo con la situación.

Políticas Relacionadas: ["Responsabilidades del Custodio de la Información"](#) y ["Remoción de Información Sensible en Papel"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

33. Divulgación de Información Desclasificada

Política: La información sensible aparentemente desclasificada o degradada porque llegó su fecha de vencimiento, no debe divulgarse a otras personas hasta que su desclasificación o degradación se confirme con el Propietario designado de la información.

Comentario: Esta política evita que las personas en posesión de datos sensibles los divulguen a otros, basando su decisión solamente en que la fecha de vencimiento llegó y pasó. La persona que posea esta información debe confirmar que dicha información ha sido degradada o desclasificada, y sólo después de ello

puede divulgarla. Esta política es una garantía porque la fecha de vencimiento pudo haberse pospuesto, pero la persona que posee copia de la información puede no haber recibido la notificación. Sin un proceso de confirmación como el descrito en esta política, la persona que posee la información podría divulgar prematuramente la información sensible con consecuencias probablemente serias. Las palabras "Propietario designado de la información" podrían ser cambiadas por "Propietario designado de la información o su delegado".

Políticas Relacionadas: "Prórroga para la Desclasificación"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

34. Medios de Almacenamiento de Información Sensible

Política: Antes de que cualquier medio de almacenamiento se envíe al proveedor, bien sea como parte de pago, para servicio o para su disposición, toda información sensible de la Empresa X debe ser destruida u ocultada de acuerdo a los métodos autorizados por el departamento de Seguridad Informática.

Comentario: Esta política garantiza la no divulgación de información sensible a personas no autorizadas que trabajan para proveedores u otros terceros. Por ejemplo, si un disco duro se tranca, puede ser enviado al proveedor para su reparación. La compañía de servicios podría examinar los datos contenidos en el disco, quizás teniendo así una divulgación no autorizada de información sensible. Para contrarrestar este riesgo, el disco duro puede ser desmagnetizado antes de enviarlo al proveedor de servicios. Los datos contenidos en el disco se pierden, lo cual es una desventaja de esta política. Esta destrucción de información confidencial sólo tiene sentido si la información ha sido respaldada adecuadamente o si las consecuencias de la divulgación son importantes. Esta política debe estar acompañada por políticas de respaldo de la información. Una alternativa más práctica es requerir que todos los discos duros que almacenan información confidencial estén cifrados, en cuyo caso no existe problema al enviarlo al proveedor de servicios. Es por esto que la palabra "ocultada" se incluye en esta política adicionalmente a la palabra "destruida". Otra alternativa es requerir acuerdos de confidencialidad a todos los terceros. La política no se aplica a CD-ROM y otros medios de almacenamiento que no puedan ser modificados, ni

tampoco se aplica a medios que no contengan información sensible. Esta política asume que el término "sensible" ha sido definido en otra política.

Políticas Relacionadas: "Respaldo de Datos," "Clasificación de Datos en Cuatro Categorías," "Transferencia de Información Sensible," y "Liberación de Componentes Usados"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

35. Etiquetado de Productos y Servicios Peligrosos

Política: Todos los productos y servicios de la Empresa X que representen un peligro para los consumidores, trabajadores o a personas involucradas, deben tener etiquetas identificando la naturaleza del peligro, formas de evitarlo y pasos a seguir en caso de que la situación cause pérdidas.

Comentario: Esta política evita problemas, tales como demandas, reclamos sindicales y de seguros de salud provenientes de accidentes de trabajadores. Es mejor notificar a las personas que ser llamado para defenderse de las demandas en las cuales alegan que se hicieron daño porque no sabían sobre los posibles peligros. Esta política también se aplica a servicios. Por ejemplo, un servicio de teléfono puede tener un mensaje saliente que advierte a los que llaman sobre la naturaleza del servicio, y les da la oportunidad de colgar sin que les sea cargada la llamada. Esta política requiere discusiones extensas con el consejero legal interno.

Políticas Relacionadas: "Mensaje de Advertencia en Inicio de Sesión"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

36. Etiquetado de Datos Usados Como Base de Decisión Gerencial

Política: Todos los datos utilizados para decisiones gerenciales que involucren cantidades por encima de los \$100.000,00 deben estar etiquetados con su origen y fecha correspondiente.

Comentario: Esta política requiere información explicativa especial cada vez que se tome una decisión gerencial importante. Tener un punto de corte reduce el costo total de reunir o generar información explicativa especial. Una política similar es apropiada para todos

los datos descargados de un computador multiusuario a un computador más pequeño. Si la gerencia no está en conocimiento del movimiento de datos de máquina a máquina, se toman decisiones asumiendo que la información es actualizada o correcta, cuando en realidad no lo es. Esta política se refiere a un malentendido común: si la información proviene de un computador, entonces debe ser información actualizada y correcta.

Políticas Relacionadas:“Etiquetado de la Propiedad Intelectual”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

37. Información Incompleta u Obsoleta

Política: Toda información obsoleta o incompleta debe ser suprimida y no distribuida a los usuarios, a menos que esté acompañada de una explicación que describa el estatus de la información.

Comentario:Esta política garantiza que los consumidores de información estarán en conocimiento de la naturaleza de la información que reciben. Si los consumidores no están en conocimiento de que cierta información es obsoleta o incompleta, pueden tomar decisiones erróneas. Esta política brinda al proveedor de información la opción de suprimirla o explicar sus deficiencias. El autor de esta política pudiera adornarla, añadiendo definiciones para los términos "obsoleta" o "incompleta". Otro cambio puede requerir que al existir dudas con respecto a la obsolescencia o al estado incompleto de la información, entonces el proveedor de la información debe dar una explicación.

Políticas Relacionadas:“Atributos de la Integridad de la Información” y “Representaciones de la Organización”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

38. Documentos Oficiales Preparados a Mano

Política: Todos los documentos oficiales de la Empresa X preparados a mano, deben utilizar tinta imborrable y si alguna entrada requiere corrección, esa entrada debe ser tachada, firmada y fechada por el originador.

Comentario:Esta política evita modificaciones no autorizadas o no detectadas a documentos en papel. La política se aplica sin importar que los documentos en

papel se utilicen más tarde como un documento fuente de entrada al computador. La política puede ser ampliada para decir que es importante que los documentos en alguna forma se preparen a mano. Por tal motivo, la política cubre la firma de lo que de otra manera sería un documento mecanografiado o impreso. Esta política establece cuál es el documento original y cuál es la copia. Desde el punto de vista legal, ésta es una distinción importante.

Políticas Relacionadas:“Prevención del Copiado de Documentos Sensibles” y “Retención del Documento Fuente”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

39. Fotografías Alteradas

Política: Toda fotografía que haya sido alterada debe estar etiquetada para indicar que se han efectuado modificaciones.

Comentario:La sofisticación del proceso para mejorar fotografías por computadores hace muy difícil, cuando no imposible, determinar visualmente si una fotografía ha sido modificada. Esto ha llevado a un gran número de abusos en los medios noticiosos, algunos de los cuales han resultado demandados. La política puede ser modificada para decir "No modifique fotos a menos que la modificación sea obvia o a menos que se notifique a las personas correspondientes". Las fotos merecen una especial mención porque es muy fácil para cualquier persona hacer esas modificaciones, y porque las fotos han sido históricamente utilizadas como una manera de demostrar la realidad. La política es relevante para todas las publicidades y otras representaciones públicas, no sólo para los medios noticiosos.

Políticas Relacionadas:“Divulgación de las Modificaciones a la Información” y “Capacidad de Reconstrucción de Cambios en Producción”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

40. Eliminación de la Información de Pago

Política: La eliminación de todos los documentos en papel que contengan información de pagos, tales como números de cuentas bancarias o de tarjetas de crédito, deben ser realizadas con máquinas trituradoras de papel o cualquier otro método autorizado de destrucción.

Comentario: Esta política evita que la información sobre pagos caiga en manos equivocadas que puedan utilizarla para cometer delitos. Quizás el ejemplo más contundente es el cargo en tarjetas de crédito, cuyos números son usualmente sustraídos de los recibos desechados en potes de basura y utilizados para hacer pedidos por teléfono. Muchos negocios botan la información de pago sin destruirla adecuadamente. Si no se utiliza este método de destrucción, lo que ponga al descubierto una investigación podría ser difícil de explicar a los clientes. También podría convertirse en un problema legal o de relaciones públicas. Esta política podría complementarse requiriendo hacer trizas la

información sensible. Esta política también evita el fraude de identidad, donde una persona no autorizada se hace pasar por otra con el propósito de obtener tarjetas de crédito, préstamos u otros beneficios utilizando la buena reputación de aquella otra persona.

Políticas Relacionadas: “Copias Sobrantes de Información Sensible,” “Período de Retención del Documento Fuente,” y “Acceso a la Información Personal”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6 EL PERSONAL

6.01 La Seguridad en Definiciones de Trabajo y Contratación

6.01.01 Inclusión de la Seguridad en las Responsabilidades del Cargo

1. Descripción del Cargo

Política: Deben incorporarse las responsabilidades específicas sobre la seguridad informática en todas las descripciones de cargo donde los trabajadores tengan acceso a información confidencial, valiosa o crítica.

Comentario: Esta política requiere que la gerencia reconozca las responsabilidades de seguridad informática en todas las descripciones de cargo de aquellos trabajadores que manejen información confidencial, valiosa o crítica. Si las descripciones de cargo contienen estas responsabilidades y los trabajadores ven que las promociones y aumentos de salarios se relacionan con la seguridad informática, sentirán más estímulo para tomar estas responsabilidades con seriedad. Las palabras "acceso a información confidencial, valiosa o crítica" podrían ser cambiadas por "manejo o utilización de los sistemas informáticos de la Empresa X". Esta política asume la existencia de un sistema de clasificación de datos. En algunas organizaciones, sería apropiado omitir las palabras "valiosa o crítica" porque solamente se dispone de un esquema de rangos de sensibilidad, tal como una política de clasificación de datos.

Políticas Relacionadas: ["Clasificación de Datos en Cuatro Categorías"](#) y ["Evaluaciones de Desempeño"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Evaluaciones de Desempeño

Política: Se debe considerar el cumplimiento de las políticas y procedimientos de seguridad informática en todas las evaluaciones de desempeño de los empleados.

Comentario: Esta política requiere que la gerencia decida, al momento de hacer las evaluaciones, si el empleado tiene alguna responsabilidad sobre seguridad informática y, si la respuesta es sí, debe determinar si el empleado ha acatado la política y los procedimientos. Esta política se refiere directamente a la actividad de evaluación de los empleados que hace la gerencia y sólo indirectamente a las bases del desempeño del empleado en el cumplimiento de la política y los procedimientos. Sin embargo, implica que la gerencia tiene expectativas en ambos casos. Las palabras "políticas y procedimientos de seguridad informática" pueden ser cambiadas por "requerimientos de seguridad informática" u otro término genérico utilizado en la organización.

Políticas Relacionadas: ["Responsabilidad en la Seguridad Informática"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6.01.02 Selección de Personal y la Política

1. Información de Empleado Potencial

Política: No se debe recopilar información personal sobre un empleado potencial, a menos que ésta sea necesaria para tomar decisiones pertinentes al cargo.

Comentario: Esta política sostiene la privacidad de los posibles nuevos empleados y mantiene los registros de personal en orden. Esta política evita reclamos sobre discriminación ilegal. Si una organización no recopila cierta información, entonces es imposible que la organización haya utilizado esa información para tomar la decisión sobre emplear o no. Esta política no puede

ser utilizada para defenderse de reclamos de discriminación basados en raza, sexo u otros atributos que son fácilmente observables y para los cuales no es necesario recolectar información adicional. Indirectamente la política promueve la identificación de la información importante para tomar la decisión de emplear y es deseable porque documenta el criterio utilizado para tomar la decisión. Debido a que esta política depende de las leyes y reglamentos locales, se debe consultar con un abogado antes de emitirla. La política puede ser ampliada para establecer los tipos de información que no se deben recaudar. Esta política permite la recopilación de información de desempeño actual en los

casos cuando el empleado solicita una transferencia. Esta política también evita que los empleados obtengan un poder no deseado con información que puedan usar para dañar la reputación de algún individuo. Algunas organizaciones pueden prohibir la retención de tal información si la decisión para la cual se aplicaba ya se tomó, aunque ciertas consideraciones legales como las ordenanzas de limitaciones se deben consultar con el consejero legal interno. Políticas como ésta realzan la moral del empleado, indicando que el patrono sí se preocupa por su bienestar. La política también ayuda a limitar la exposición del patrono a acusaciones sobre la invasión de la privacidad de ciertos individuos.

Políticas Relacionadas: “Notificación de Monitoreo Electrónico del Desempeño” y “Pruebas de Honestidad y Estabilidad Emocional”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Verificaciones de Historia Crediticia de Empleados Potenciales

Política: Se debe notificar a todos los candidatos si sus referencias crediticias o sus antecedentes serán investigados como parte del proceso de reclutamiento y selección, y deben recibir la oportunidad de retirar su solicitud de empleo si no desean que la Empresa X conozca dicha información personal.

Comentario: Esta política da a los empleados en potencia la oportunidad de decidir revelar cierta información personal a su futuro empleador. Si deciden no revelar tal información, ellos mismos se retiran de la competencia por el empleo. Otro objetivo cumplido por esta política es que los empleados en potencia saben cuál información está siendo utilizada para tomar una decisión sobre ellos. Esto permite que el candidato investigue si cree que una información errónea fue la que causó una decisión desfavorable. Con esta política se tiene la noción que los individuos son los que finalmente tiene el control del flujo de su información personal. Esta política puede ser ampliada para incluir clientes y terceros, en cuyo caso se les debe informar de todos los datos personales utilizados para tomar decisiones sobre ellos. Una compañía aseguradora de salud, cuando tome la decisión de otorgar o no una póliza, puede utilizar este procedimiento. Los bancos crecientemente utilizan este procedimiento para decidir si otorgan un préstamo, como por ejemplo una hipoteca.

Políticas Relacionadas: “Distribución de los Registros del Personal” y “Huellas Digitales de Empleados”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Información Sobre Estilo de Vida del Empleado Potencial

Política: Los candidatos a emplearse con la Empresa X no deben estar supeditados a exámenes que revelen su estilo de vida, su afiliación política o preferencias religiosas, a menos que esta información sea necesaria para determinar si el candidato es adecuado para el cargo.

Comentario: Esta política evita que una organización utilice exámenes para determinar la información sobre los candidatos que ellos mismos no han querido revelar. La política protege la privacidad de los individuos que solicitan un cargo y, potencialmente, evita que la Empresa X sea demandada o reciba publicidad adversa. La política restringe el uso de exámenes a aquéllos directamente relacionados con el trabajo. Los exámenes sicológicos que demuestran la inclinación al robo de algunos empleados son de especial interés para la mayoría de los patronos. Estos exámenes son consistentes con la forma en que se redactó la política porque la honestidad puede ser considerada como un requerimiento para ciertos trabajos, como el de cajero.

Políticas Relacionadas: “Cargos de Confianza en el Área de Computación”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4. Divulgación de Información a Solicitantes de Empleo

Política: Los detalles técnicos de sistemas informáticos tales como direcciones de redes, diagramas de redes y software de seguridad utilizado, no deben ser revelados a los aspirantes al empleo mientras no hayan firmado un acuerdo de confidencialidad y también hasta que hayan sido empleados o contratados.

Comentario: Esta política evita el uso de un nuevo tipo de ataque, en el cual la persona se hace pasar por un aspirante a un trabajo técnico en sistemas informáticos. El entrevistador hará una serie de preguntas técnicas sobre el ambiente de computación, para determinar si el solicitante tiene las destrezas para el puesto. En el proceso, el atacante obtendrá información útil que puede

utilizarse con ingeniería social para montar un ataque más preciso. Esta política considera a los aspirantes como terceros no confiables.

Políticas Relacionadas: “Entrega de Documentación de Sistemas” y “Convenios de Intercambio de Software y Datos”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Re-empleo de Empleados Despedidos

Política: No deben reengancharse o contratarse ex-empleados, ex-consultores y ex-contratistas despedidos, sin el consentimiento de un vicepresidente ejecutivo.

Comentario: Entre otras cosas, esta política evita que empleados despedidos se conviertan en consultores o contratistas de la Empresa X. Debido a que estos individuos pueden sentir rencores hacia la organización, es conveniente evitar ubicarlos en posiciones de confianza en la que podrían ocasionar serios daños. Otra intención de esta política es netamente económica. Algunos técnicos especialistas en computación que se saben indispensables, renuncian y solicitan a sus ex-empleadores que los contraten como consultores con un salario mucho más alto. Esta política es disuasiva de tales manipulaciones. Algunas organizaciones llevan esta política un paso más allá, indicando que toda persona despedida por cualquier razón, no debe ser empleada o contratada. En ciudades pequeñas y otras áreas donde el número de personal técnico es limitado, esta versión estricta de la política puede evitar, sin embargo, que la Empresa X utilice el talento local disponible. En algunas industrias es normal que el personal se vaya algunos años y luego regrese, lo que hace que esta política no sea adecuada para estas industrias.

Políticas Relacionadas: “Período de Prueba Para Trabajadores Nuevos”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Período de Prueba Para Trabajadores Nuevos

Política: Todos los nuevos trabajadores y aquéllos que hayan sido re-empleados o contratados después de una evaluación poco satisfactoria de su desempeño, deben ser colocados en un período de prueba de seis meses

durante el cual la gerencia a quienes reportan debe seguir atentamente su desempeño y actitud, con el propósito de tomar la decisión de retenerlos o despedirlos.

Comentario: Esta política brinda a la gerencia un período suficiente de tiempo para evaluar el desempeño de los empleados, y les permite despedirlos basándose en el mal desempeño, en su negativa a seguir los controles internos o porque de alguna forma no son considerados idóneos. La política notifica a la gerencia que deben monitorear con cuidado el trabajo de estas personas para garantizar que son integrantes idóneos de la organización. Con mucha frecuencia la gerencia no llega a conocer a sus subordinados. Esto puede provocar en muchas ocasiones problemas de seguridad. Por ejemplo, si un empleado tiene un problema de deudas de juego y debe obtener dinero rápidamente para pagar una deuda vencida, puede cometer una estafa computarizada. Si la gerencia conoce de este problema, puede referir confidencialmente al empleado a un consejero psicológico o sugerir otras medidas para remediar la situación. Una política como ésta también otorga flexibilidad adicional a la gerencia si despidie al empleado dentro de los seis meses de prueba, lo cual puede disuadirlo de demandar o reclamar. El tiempo del período de prueba puede variar dependiendo de la organización.

Políticas Relacionadas: “Re-empleo de Empleados Despedidos”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

7. Fianzas de Trabajadores

Política: Todos los trabajadores con cargos de confianza particularmente en el área de computación deben contar con una fianza por un mínimo de \$1.000.000.

Comentario: La fianza es un tipo de póliza de seguro contra delitos como estafas, desfalcos y espionaje industrial. Las fianzas a veces se conocen con el nombre de "fianza de fidelidad" o "póliza de fidelidad". El proceso de obtener una fianza para una persona en una posición de confianza normalmente requiere de una investigación de sus antecedentes. Esto puede ser un proceso demostrativo en el cual la gerencia se forma una idea de la historia de la persona. Utilizando la información de los antecedentes, la gerencia estará más capacitada para tomar decisiones sobre el grado de confianza que se puede dar al individuo. Aunque la

investigación no revele algo que pueda indicar problemas, la fianza contra pérdidas sufraga los costos de cualquier problema que se pueda presentar. Dichas investigaciones de los antecedentes dan una idea a la gerencia del alcance hasta dónde ciertas personas tienen en sus manos el futuro de la organización. El conocer que se hacen investigaciones sobre sus antecedentes evita que algunas personas no idóneas soliciten trabajos que involucran un alto grado de confianza. Algunos procesos de cobertura de seguros requieren que las empresas obtengan fianzas para ciertos tipos de empleados.

Políticas Relacionadas: “[Información Sensible en Pequeños Computadores](#),” “[Información Sobre Estilo de Vida del Empleado Potencial](#),” “[Revisión de Antecedentes](#),” y “[Cargos de Confianza en el Área de Computación](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

8. Trabajo en Proyectos Sensibles

Política: Sólo empleados con desempeño de bueno a excelente y con antigüedad de por lo menos dos años en la Empresa X, pueden trabajar en el desarrollo de nuevos productos y otros proyectos de alta sensibilidad.

Comentario: Esta política define quiénes pueden trabajar con la información más confidencial, limitando los cargos a aquéllos menos propensos a caer en sobornos, ser manipulados por un espía industrial o aprovecharse de su posición para obtener información para luego venderla fuera de la Empresa X. El período de espera de dos años hace más difícil que los espías industriales consigan un empleo en la Empresa X sólo para tener acceso a la información. La política también tiene la intención de evitar que personas bajo presión, sea ésta financiera o de otro tipo, trabajen en proyectos donde pueden tener acceso a la información más sensible. La política también justifica otra investigación de antecedentes antes de que un empleado sea asignado a un proyecto que involucra el manejo de la información más sensible. La política convierte en un honor el trabajar en estos proyectos. Esto induce a una mayor fidelidad y adicionalmente aísla a la Empresa X de ataques de ingeniería social como los mencionados anteriormente. Habrá ocasiones cuando se necesite pericia especializada externa para completar un proyecto. En esos casos se autoriza una desviación de esta política. Esta política es solamente apropiada para organizaciones relativamente grandes y bien establecidas.

Políticas Relacionadas: “[Identificadores de Usuario para Terceros](#)” y “[Verificaciones de Historia Crediticia de Empleados Potenciales](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

9. Convictos Violentos

Política: No deben hacerse ofertas de trabajo a individuos que hayan sido condenados judicialmente por crímenes violentos que, de repetirse, representarían un daño físico para los empleados o la propiedad de la Empresa X.

Comentario: Esta política garantiza que la fuerza laboral estará compuesta de empleados seguros y respetuosos de las leyes. La política también asegura que los trabajadores no estarán indebidamente expuestos a la violencia en el trabajo. Si la gerencia, en pleno conocimiento, emplea a dicha persona y esa persona daña a otro empleado, la gerencia es considerada responsable del daño. Los empleados seguros también son menos propensos a dañar sistemas de computación y comunicaciones en ataques de ira. Por ejemplo, un usuario disparó a una pantalla y otro golpeó con una mandarria su estación de trabajo. Esta política puede ser ampliada para incluir contratistas, consultores, temporales y otros, además de los empleados de la Empresa X.

Políticas Relacionadas: “[Cargos de Confianza en el Área de Computación](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

10. Cargos de Confianza en el Área de Computación

Política: Las personas que hayan sido condenadas por delitos judiciales no deben ser empleados, contratados, promovidos o mantenidos en cargos de confianza en el área de computación.

Comentario: Esta política asegura que las personas de quienes depende la Empresa X son verdaderamente confiables. A pesar de que muchas personas no están de acuerdo, argumentando que esta política no da a los delincuentes convictos la oportunidad de reintegrarse al resto de la sociedad, la política es firme en cuanto a no emplear a quienes no son confiables. Si fuese redactada abiertamente como está, esta política puede ser restringida a delitos que tengan relación con el trabajo

que la persona va a realizar. Por ejemplo, los bancos no emplearían a un cajero condenado por delitos de fraude o robo, pero podrían emplear a una persona convicta del delito de manejar vehículos bajo la influencia del alcohol. Alternativamente, esta política pudiera ser restringida a convictos de delitos que muestren falta de honradez o falta de confianza. Por ejemplo, una compañía grande de computación empleó a un individuo que había sido convicto de fraude de cuello blanco para el cargo de gerente de Seguridad Informática y esto, a las claras, es una violación de la política. Otra variación de esta política es restringirla a trabajadores que tendrán acceso a información confidencial, crítica o valiosa. La política aquí descrita implica que se debe realizar una investigación de antecedentes para determinar si el individuo tiene prontuario policial.

Políticas Relacionadas: “Convictos Violentos,” “Revisión de Antecedentes,” “Fianzas de Trabajadores,” e “Información Sobre Estilo de Vida del Empleado Potencial”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

11. Revisión de Antecedentes

Política: Todos los trabajadores en consideración para ser colocados en posiciones de confianza en el área de computación deben pasar la revisión de antecedentes, la cual incluye la verificación de prontuarios policiales, demandas, problemas crediticios, multas de tránsito y empleos anteriores.

Comentario: Esta política informa a la gerencia que deben conocer a quienes están empleando o contratando. Por ejemplo, si una investigación de antecedentes revela que un individuo tiene una historia de robo bancario, la gerencia puede reconsiderar la decisión de emplearlo. Muchas veces los delincuentes de computación no son enjuiciados y continúan haciendo de las suyas con el nuevo patrono. Mientras que las leyes de privacidad restringen lo que el empleador puede decir acerca de su ex-empleado, aquéllos que llevan a cabo las investigaciones de antecedentes muchas veces recogen las reservas que hay sobre el individuo. A menudo, la pregunta de si el ex-empleado volvería a emplear al individuo es suficiente para dar una panorámica del estatus de dicho ex-trabajador. Aun sin los detalles, la reserva mostrada es suficiente para descalificar a un candidato o motivo para realizar más investigaciones. Este proceso a veces se denomina obtener referencias del carácter y también

puede ser añadido a la política. Otras cosas que pudiesen agregarse a la lista de tareas que deben efectuarse son: verificación de lo completo y exacto de su currículum, la confirmación de aptitudes académicas y profesionales, la verificación de que el solicitante es ciudadano o extranjero legal y la verificación de la identidad a través de su pasaporte o licencia de conducir. Algunas organizaciones evitan mencionar los tipos de investigaciones de antecedentes que se harán, y sólo dicen "se hará una investigación de antecedentes de acuerdo con las procedimientos normales de la empresa". En este caso, un memo separado del departamento de Recursos Humanos puede delinejar los tipos de investigaciones necesarias para los diferentes cargos. Este procedimiento brinda a la gerencia flexibilidad adicional para determinar las investigaciones que se harán para cada cargo disponible.

Políticas Relacionadas: “Cargos de Confianza en el Área de Computación,” “Informe de Cambios en Situación,” y “Fianzas de Trabajadores”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

12. Pruebas con Polígrafos

Política: Todos los trabajadores de la Empresa X en consideración para ser colocados en posiciones de confianza en el área de computación, deben pasar la prueba del polígrafo antes de comenzar a trabajar en su nueva posición.

Comentario: Esta política garantiza que los administradores de sistemas, de redes y de seguridad pasarán la prueba de detección de mentiras antes de recibir acceso a los poderosos privilegios informáticos. La política se aplica a aquéllos que tienen acceso a información altamente restringida, no sólo a los que trabajan en posiciones de tecnología de información. La política está escrita de manera deliberadamente general, para cubrir ambos tipos de trabajador. Puede ser que las personas no pasen el detector de mentiras sin estar mintiendo, lo que sucede es que las máquinas son efectivas en un 85-95% para pruebas específicas. Si la organización adopta esta política tan estricta, necesita tener un procedimiento para resolver los casos cuando la persona falla la prueba, pero alega estar diciendo la verdad. Finalmente, la política involucra pruebas solamente cuando se emplea personal nuevo, aunque puede ser ampliada para incluir pruebas periódicas a pesar de ser costoso.

Políticas Relacionadas: “[Fianzas de Trabajadores](#)” y “[Verificaciones de Historia Crediticia de Empleados Potenciales](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

13. Acceso a Información Privada

Política: Los empleados deben pasar una investigación de antecedentes antes de recibir el acceso a información privada.

Comentario: Esta política requiere una revisión de antecedentes adicional a la efectuada en su verificación de pre-empleo, para cada trabajador que tendrá acceso a información personal o privada. Esta política estipula que sólo un grupo restringido de personal debe tener acceso a ese tipo de información. Un empleado temporal o voluntario no debe tener acceso a datos privados a menos que apruebe la verificación adicional de sus antecedentes. La política asume que la organización ya ha definido cuáles datos son privados. La política no dice nada sobre los componentes de la investigación, pero los mismos deben ser documentados en un procedimiento aparte. Esta política es apropiada para un hospital, una clínica, una compañía de seguros de salud o cualquier otra organización que actúe como Custodio de datos privados que van más allá de registros laborales. Si las palabras "información privada" fuesen cambiadas para "información patentada", entonces la política sería apropiada para una gran cantidad de organizaciones comerciales, tales como compañías de computación de alta tecnología, farmacéuticas y de exploración petrolera.

Políticas Relacionadas: “[Revisión de Antecedentes](#)” e “[Integridad del Registro Personal](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

14. Información Sensible de Productos

Política: Todos los trabajadores que tendrán acceso a información sensible de productos, tales como planes de mercadeo, especificaciones de ingeniería o procedimientos de manufactura, deben pasar la investigación normal de antecedentes efectuada por el departamento de Recursos Humanos.

Comentario: Esta política selecciona los secretos industriales u otra información que pertenezca a la Empresa, y otorga el acceso a información sensible sólo

a los trabajadores que han pasado las investigaciones de antecedentes. Esta investigación ayudar a eliminar a ciertos individuos que representan un riesgo que no vale la pena correr. Por ejemplo, una investigación de antecedentes puede revelar que un solicitante recientemente trabajó para un competidor, lo cual puede desanimar a la gerencia en el sentido de darle acceso a información sensible del producto. Esta política está orientada hacia las organizaciones del sector privado que ofrecen un producto. La política puede ser ampliada para incluir toda la información que tiene un grado de sensibilidad designado, quizás "secreto" y si se alterase, sólo imitaría las políticas normales típicas de las organizaciones militares. Si la política se amplía para enlazarla con las etiquetas de clasificación de datos, entonces se necesita otra política que describa el sistema de clasificación de datos. Esta política se aplica por igual a contratistas, consultores, temporales, internos y voluntarios, así como a los empleados. La palabra "información de producto", como se usa aquí, se refiere no sólo a los productos nuevos y no publicados, sino también a la información sobre los productos existentes.

Políticas Relacionadas: “[Acuerdos de Confidencialidad — Organización](#)” e “[Identificadores de Usuario para Terceros](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

15. Huellas Digitales de Empleados

Política: Antes de comenzar a trabajar, se deben tomar las huellas digitales de los empleados potenciales que tendrán acceso a información sensible, las cuales se utilizarán para determinar si el empleado potencial posee prontuario policial.

Comentario: Esta política obtiene datos específicos de identificación sobre individuos, que pueden ser comparados con la base de datos gubernamental de delincuentes conocidos. Esta política requiere una investigación de antecedentes a nivel nacional, mientras que la verificación local de antecedentes penales está restringida a la base de datos regional. En algunos casos es necesaria una investigación internacional de los antecedentes. Esta política puede ampliarse para incluir a consultores, contratistas, temporales y otros que no son empleados regulares. Las palabras "información sensible" también puede ampliarse a "información confidencial, crítica o valiosa", e igualmente incluir a aquéllos promovidos o transferidos a posiciones y no

sólo los nuevos empleados. Para garantizar que esta política no cause problemas con los trabajadores, se deben dar las explicaciones necesarias.

Políticas Relacionadas: “[Fianzas de Trabajadores](#)”, “[Verificaciones de Historia Crediticia de Empleados Potenciales](#)”, e “[Iniciación de Transacciones en Computadores](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

16. Pruebas de Honestidad y Estabilidad Emocional

Política: Todos los trabajadores en consideración para ocupar posiciones de confianza en computación deben pasar las pruebas de honestidad y estabilidad emocional autorizadas por el departamento de Recursos Humanos.

Comentario: Esta política garantiza que la baja gerencia aplicará pruebas que aseguren que los trabajadores que serán ubicados en posiciones de confianza en computación merecen dicha confianza. Estas pruebas pueden ser escritas, entrevistas de preguntas y repuestas, estudios de casos u otros tipos de prueba. Estudios estadísticos demuestran que estas pruebas representan maneras eficaces y justas de determinar la honestidad. Las pruebas son crecientemente utilizadas como una manera de garantizar que un trabajador potencial actuará como se espera de él, particularmente cuando esté trabajando bajo presión o en circunstancias adversas. Estas pruebas permiten al empleador retener trabajadores que son menos propensos a cometer estafas de computación, o de vengarse destruyendo datos. Esas pruebas a veces son eufemísticamente llamadas pruebas de actitud.

Políticas Relacionadas: “[Información de Empleado Potencial](#)” y “[Huellas Digitales de Empleados](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

17. Revisión de Antecedentes de No Empleados

Política: Los empleados temporales, los consultores, los contratistas y el personal de organizaciones externas no deben recibir acceso a información sensible o acceso a sistemas de información crítica, a menos que pasen por una verificación de antecedentes proporcional a las efectuadas a los empleados regulares.

Comentario: Esta política garantiza que los gerentes departamentales y gerentes de proyectos no evadirán el proceso de verificación de antecedentes exigido para todos los empleados. Con el fin de apresurar el trabajo y reducir costos, los gerentes medios de las organizaciones contratan externamente una variedad de actividades que con frecuencia implican privilegios importantes en el sistema o acceso a información sensible. Tal vez la mayor preocupación es la reciente contratación externa de trabajos de programación de computadores para aplicaciones críticas. Frecuentemente estas contrataciones de desarrollo de código se envían a países extranjeros donde trabajan personas cuyas lealtades e intenciones se desconocen. Este tema es preocupante, ahora que el terrorismo se ha convertido en un problema mundial. Esta política conlleva una precaución adicional a la tendencia de contratar externamente toda actividad, excepto aquéllas directamente relacionadas con el núcleo de la empresa. En algunos casos la organización que adopta esta política se apoya en verificaciones de antecedentes efectuadas por terceros, tales como organizaciones de reclutamiento.

Políticas Relacionadas: “[Identificadores de Usuario para Terceros](#)” y “[Privilegios de Trabajadores Temporales](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

18. Extranjeros

Política: No deben trabajar extranjeros en los sistemas informáticos de la Empresa X .

Comentario: Esta política garantiza que las personas que trabajan en sistemas informáticos internos son dignas de confianza. Un buen número de casos de la vida real ha demostrado que algunos extranjeros realizan trabajos en sistemas informáticos con miras a comprometerse en espionaje industrial o información militar. Esta política no se debe interpretar con una condena a todos los extranjeros o aquéllos que están en proceso de convertirse en ciudadanos. Si los trabajadores residen en el país en el cual trabajan, al menos estarán sujetos a las leyes de ese país. Sin embargo, si los empleados se van a ir pronto, pueden sentirse menos inclinados a acatar las leyes, políticas, y otras reglas de dicho país. Esta política reconoce que los sistemas informáticos se han convertido en críticos para las organizaciones y que no cualquier persona puede trabajar en estos sistemas informáticos. Esta política es consistente con el criterio militar del proceso de certificación de seguridad, pero también es aplicable al sector

privado. Se debe ser cuidadoso para garantizar que esta política no es ilegal de conformidad con las leyes anti-discriminatorias de la jurisdicción respectiva.

Políticas Relacionadas: “Transporte Internacional de Información Secreta — Seguridad” y “Revisión de Antecedentes”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

19. Antiguos Hackers y Delincuentes Reformados

Política: La Empresa X no debe emplear antiguos hackers ni delincuentes reformados para trabajar en seguridad informática o realizar trabajos forenses.

Comentario: Esta política proporciona una clara e inequívoca guía de reclutamiento a la gerencia. Al emplear a ex-hackers o delincuentes reformados se asume el riesgo que estas personas vuelvan a traicionar la confianza dada. Esta política de ninguna manera evita que la gerencia emplee a un consultor para hacer un ataque de penetración. Esta evaluación de riesgo es ahora un enfoque legítimo para descubrir vulnerabilidades. Esta política sólo limita el tipo de persona que puede ejecutar tal servicio. Algunas veces, el término “hacker de sombrero blanco” es usado para un profesional que ejecuta servicios legítimos de ataques

de penetración, mientras el término “hacker de sombrero negro” es usado para un intruso oculto con antecedentes cuestionables.

Políticas Relacionadas: “Equipos de Investigación de Seguridad Informática” y “Conflictos de Intereses”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

20. Aumento Significativo de Riqueza

Política: En caso de que un trabajador de la Empresa X demuestre un inexplicable aumento de riqueza, la gerencia tiene el deber de investigar discretamente el origen de dicha nueva riqueza.

Comentario: Esta política informa a la gerencia local que los aumentos inexplicables y significativos de riqueza pueden señalar fraude interno. Si ocurriese un cambio así, la gerencia debería entrevistar al trabajador correspondiente e investigar los privilegios y accesos a los fondos de la organización. Aun cuando debe haber respeto hacia la privacidad del individuo, este cambio de riqueza es a veces un indicador válido de que algo está fuera de lugar.

Políticas Relacionadas: “Trabajadores Como Clientes” e “Investigación de Delito Computarizado”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6.01.03 Acuerdos de Confidencialidad

1. Derechos de Propiedad

Política: Sin excepciones específicas escritas, todos los programas y la documentación generados o proporcionados por cualquier trabajador en beneficio de la Empresa X son propiedad de la Empresa X y todos los trabajadores que proporcionen tales programas o documentación deben firmar una declaración a tal efecto, previa a la entrega de dichos materiales.

Comentario: Son frecuentes las controversias sobre la propiedad de los programas y la documentación. Los programadores reclaman que tienen el derecho de llevarse sus creaciones a su nuevo empleo o a clientes consultores externos. Los patronos argumentan que dichos materiales son producto del trabajo para el cual fue empleado y, como tal, son propiedad del Empleador. Esta política clarifica esta área y da a la Empresa X

influencia en cualquier disputa relacionada, sea interna o en materia juzgada en tribunal. Esta política notifica a los programadores y trabajadores relacionados sobre los derechos de propiedad. En este caso, la primera mitad de la declaración de la política es suficiente pero las organizaciones particularmente interesadas en esta materia, pueden incluir la otra mitad de lo establecido en la política, la cual tiene la intención de requerir que la gerencia lo incluya en convenios de empleo y con consultores. Esta política no es un convenio formal con un programador. Sólo exige la existencia de un convenio cuando se preparan programas y documentaciones. El lector debe contactar a un consejero interno legal para desarrollar tanto un convenio como una política como ésta, porque habrá consideraciones específicas relativas a la jurisdicción pertinente.

Políticas Relacionadas: “Convenios de No Competencia,” “Derechos de Propiedad Intelectual,” “Confidencialidad de la Documentación,” y “Recuperación de la Propiedad de la Organización”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Acuerdos de Confidencialidad — Organización

Política: Todos los empleados deben personalmente firmar un acuerdo de confidencialidad con la Empresa X antes de comenzar a trabajar, o si un trabajador ha estado trabajando sin dicho acuerdo, debe firmarlo como condición de empleo.

Comentario: La intención de esta política es evitar la divulgación de información sensible a persona alguna, a menos que dicha persona haya previamente firmado un acuerdo de confidencialidad (NDA, por sus siglas en inglés). Organizaciones en las cuales el negocio depende de la protección continua de cierta información, tal como los laboratorios de investigación, compañías de alta tecnología y organizaciones militares, sentirán que esta política es una necesidad. Cada NDA de la organización es comúnmente redactado por su departamento Legal. Un borrador NDA está incluido en un apéndice de este libro. Esta política requiere que cada individuo firme el NDA y que no firmen a nombre de toda la organización. Este requerimiento evita que individuos digan que no recibieron notificación de que la información era sensible, y que por ello no tomaron las precauciones apropiadas. No se aceptan modificaciones personales hechas al NDA por los trabajadores. Para resaltar la importancia de la confidencialidad, en algunas organizaciones, se exige a los trabajadores firmar periódicamente el NDA, aunque esto es generalmente considerado excesivamente estricto. Esta política asume que el NDA es un contrato aislado, pero puede integrarse fácilmente a los contratos de empleo, de consultoría o documentos relacionados.

Políticas Relacionadas: “Revisión de Antecedentes,” “Convenio de Cumplimiento,” “Acuerdos de Confidencialidad,” y “Acuerdos de Confidencialidad — Terceros”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Cambios en el Empleo

Política: Cuando haya cambios en la situación laboral o cambios en la condición de trabajo de un trabajador externo, como un contratista, consultor o temporal, el contenido del acuerdo de confidencialidad de la Empresa X debe ser revisado con el gerente de la persona correspondiente.

Comentario: Esta política tiene la intención de recordar a los trabajadores que ellos firmaron un acuerdo de confidencialidad, y que la Empresa X intenta mantenerlos comprometidos con dichos términos y condiciones. Aunque normalmente es parte de una entrevista de despedida, la revisión de los términos y condiciones del acuerdo de confidencialidad no debe tomar mucho tiempo. La política, tal y como está redactada, es deliberadamente ambigua acerca de las palabras exactas que debe decir el gerente, dejándolo a las circunstancias y preferencias personales de cada quien. En algunos casos, el recordatorio lo hace un integrante del personal de Recursos Humanos, y no el gerente del empleado. En cualquier caso, debe mencionarse en la política el cargo de la persona que va a realizar la revisión. La existencia y el forzoso cumplimiento de esta política pueden ayudar a las organizaciones en sus esfuerzos legales por demostrar que diligentemente intentaron proteger los secretos industriales, y por tanto deben ser elegibles para recibir asistencia legal contra las pérdidas ocasionadas por el trabajador que no cumplió su parte.

Políticas Relacionadas: “Acuerdos de Confidencialidad — Organización”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Acuerdos de Confidencialidad con Antiguos Patronos

Política: Los empleados que hayan trabajado en organizaciones de la competencia deben ser alentados a respetar los acuerdos de confidencialidad que firmaron con dichas organizaciones y ningún trabajador debe presionar a estos empleados en el sentido de divulgar información que pueda ser beneficiosa para la Empresa X.

Comentario: Esta política informa claramente que la Empresa X no tiene intención de forzar a los nuevos empleados a divulgar información que es propiedad del patrono anterior. La política también indica que emplear personal de las organizaciones de la competencia no es parte de una estrategia para realizar espionaje industrial.

Esta política es muy relevante para las organizaciones donde existe alta rotación. Algunos conocimientos serán transferidos inconscientemente de una organización a otra cada vez que ocurre tal situación de reclutamiento de personal. A pesar de que lo específico del caso dominará cualquier acción legal que surja, una política como ésta será de ayuda porque demuestra que la gerencia no apoya el espionaje industrial indirecto.

Políticas Relacionadas: “[Conflictos de Intereses](#)” y “[Solicitudes de Información Organizacional](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Convenios de No Competencia

Política: Al momento de emplearse en la Empresa X, todos los empleados deben firmar un convenio de no competir con la Empresa X durante un período de seis meses después de su separación de ella.

Comentario: Los convenios de no competir básicamente impiden a los ex-trabajadores formar un negocio en competencia directa con su ex-patrono. A menudo, estos convenios se encuentran restringidos por el tiempo

y la geografía; por ejemplo, establecer un negocio en la misma ciudad no es aceptable para algunos, pero hacerlo en otra sí lo es. Los ex-empleados pueden significar un reto competitivo para su ex-patrono si roban información intelectual de la Empresa X. Los convenios de no competencia pueden ser útiles en los tribunales si se presenta un juicio sobre las acciones del ex-empleado. A pesar de que el robo de información es algo que el ex-patrono no puede comprobar en la corte, comenzar un negocio en competencia con el antiguo patrono es relativamente fácil de probar. Esta política requiere la firma de un convenio de no competencia. Se recomienda consultar con los consejeros internos legales sobre el convenio y su uso en concordancia con una política como ésta. Esta política requiere que la gerencia haga que los empleados firmen tal convenio. Es conveniente que los empleados firmen al momento de emplearse, pues en ese momento tendrán la mejor disposición para aceptar este tipo de convenio.

Políticas Relacionadas: “[Derechos de Propiedad Intelectual](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6.01.04 Términos y Condiciones de Empleo

1. Derechos de Propiedad Intelectual

Política: Mientras sean empleados de la Empresa X, todo el personal debe otorgar a la Empresa X derechos exclusivos sobre las patentes, los derechos de autor, los inventos u otra propiedad intelectual que originen o desarrollen.

Comentario: Esta política asigna al empleador los derechos a toda propiedad intelectual generada por los empleados. Algunos convenios de consultores y contratistas también contienen provisiones al efecto. Aunque generalmente no se hace, la política podría ser restringida al material que de una forma u otra está relacionado con el negocio de la Empresa X. Sin embargo, se utiliza un enfoque más general para asegurar que la Empresa X retiene la opción de aprovechar tal propiedad intelectual. Por otro lado, la política puede hacer referencia tanto a las horas de trabajo como a las horas no hábiles. Debido a la proliferación de contratación externa, es especialmente importante clarificar los derechos sobre los trabajos generados por terceros. Sin una política como ésta, los programadores en muchas ocasiones reclamarán que el código que

desarrollaron es de su propiedad. Para asegurar de que no haya malos entendidos, muchas organizaciones hacen que sus empleados firmen convenios que incluyen palabras similares a las encontradas en esta política. Ya sea un convenio o una política lo que se utilice, los lectores deben solicitar consejo interno legal en esta materia, debido a que hay consideraciones jurisdiccionales específicas. También esta política puede ser un impedimento para emplear a ciertas personas creativas que deseen retener los derechos de propiedad intelectual sobre su trabajo. La noción detrás de esta política puede ser no aceptable para algunos empleados, quienes pueden llegar a pensar que esta política es un reflejo de la potestad de la Empresa X para ser dueña de ellos y de todo lo que produzcan. Esta noción puede ser importante para las negociaciones con sindicatos y para los esfuerzos de redefinición de la cultura corporativa.

Políticas Relacionadas: “[Convenios de No Competencia](#),” “[Propiedad Intelectual Desarrollada Fuera de Sede](#),” “[Derechos de Propiedad](#),” y “[Comunicaciones Públicas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Recuperación de la Propiedad de la Organización

Política: Los empleados, los temporales, los contratistas y los consultores no deben recibir su pago final hasta que no hayan devuelto todo el hardware, software, materiales de trabajo, información confidencial y cualquier otra propiedad de la Empresa X.

Comentario: Esta política garantiza la devolución de la información confidencial, computadores personales y cualquier otra propiedad de la Empresa X. Esta política da a la Empresa X una ventaja para asegurarse de que estos materiales sean devueltos. Si un trabajador ya se ha retirado y si se le ha cancelado su último cheque, hay muy poco incentivo para que devuelva los materiales. La empresa debe mantener un registro preciso del hardware, software y otros materiales asignados a los trabajadores para que pueda recuperarlos. También son útiles las constancias escritas de propiedad firmadas por el trabajador, a la hora de recuperar estos materiales. Retener un cheque de pago es ilegal en algunas jurisdicciones, así que se debe solicitar consejo legal interno. Dado que los despidos, reducciones de personal, terminación de contrato y otras separaciones son tan comunes, hay una creciente necesidad de abordar los asuntos específicos de sistemas informáticos asociados con estos cambios laborales.

Políticas Relacionadas: “Derechos de Propiedad”, “Derechos de Propiedad Intelectual,” y “Remoción de Información Sensible”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

3. Empleados Que Viajan Conjuntamente

Política: Los empleados no deben abordar el mismo avión si ello implica que tres o más directivos, cinco o más empleados, o dos o más ingenieros del mismo departamento estarían en el mismo vuelo.

Comentario: Esta política implícitamente reconoce que uno de los más importantes activos de una organización es el conocimiento de sus empleados. La intención de la política es garantizar que un accidente aéreo no dañará la habilidad de la organización de llegar a sus metas. La política puede ser ampliada para incluir otros medios de transporte como el terrestre, pero los accidentes aéreos

son repentinos y catastróficos, donde se podría perder a varios empleados a la vez. Aunque no es común, la política puede ser ampliada para incluir actividades con riesgo de muerte, tales como utilizar planeadores y las carreras de motos. No hay nada especial sobre el número de empleados incluidos en esta política. El número de ingenieros de un departamento, por ejemplo puede ser tres. Una presunción de esta política, tal como está redactada, es que los ingenieros son empleados importantes de la organización. Si éste no fuese el caso, entonces deben efectuarse sustituciones apropiadas tales como, “especialistas en sistemas informáticos”. Esta política asume que la Empresa X es una organización relativamente grande.

Políticas Relacionadas: “Adiestramiento Multidisciplinario” e “Información de Contacto”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Informantes Internos

Política: De vez en cuando la Empresa X utiliza informantes, quienes pueden ser ubicados en diversas posiciones internas y que aparentan ser como cualquier otro trabajador, pero sin notificarles a otros trabajadores su presencia o la naturaleza del trabajo que efectúan tales informantes.

Comentario: Esta política disuade a los trabajadores de cometer delitos, abusos y otros actos contrarios a la política organizacional o las leyes locales. La utilización de informantes puede ser una ayuda valiosa para que la gerencia obtenga información acerca de las actividades que se ejecutan dentro de la organización. A pesar de que esta política no está limitada al área de seguridad informática, puede dar beneficios significativos en esa misma área. Un informante puede, por ejemplo, decirle a la gerencia que los usuarios están compartiéndose las contraseñas, que están utilizando recursos de computación de la organización para propósitos personales, o en otras palabras, están haciendo cosas indebidas. Un auditor o un consultor externo podría no ser capaz de obtener esta información ya que los trabajadores saben que un auditor o consultor preparará un reporte para el consumo de la gerencia. Una contraindicación de esta política es que puede fomentar una cultura corporativa paranoica. Esta política se utiliza de manera provechosa en las organizaciones que le dan un gran porcentaje de importancia a la honestidad y lealtad de su personal, y que tienen relativamente pocos mecanismos para detectar fraudes, desfalcos, y otros abusos.

Políticas Relacionadas:“Uso de Investigadores”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

5. Inteligencia Competitiva

Política: Cuando se recopile información sobre la competencia, el personal de la Empresa X, o cualquier persona designada para recoger dicha información en representación del personal de la Empresa X, no debe mentir nunca o falsificar su identidad.

Comentario: Esta política evita algunas prácticas cuestionables en donde la persona posa como si fuera legítimamente elegible para recibir cierta información, cuando en realidad no lo es. Esta política evita la mala publicidad que puede surgir de declaraciones públicas sobre prácticas cuestionables. En algunos casos, estas tácticas de recopilación de datos pueden considerarse fraudulentas y, por tal motivo, ilegales. Esta política se dirige a ese tipo de comportamiento, pero también cubre comportamientos que pueden no ser ilegales, en el estricto sentido de la palabra. La política aborda la posición en favor de decir la verdad y ser honesto en asuntos de negocios. La política es una restricción a las acciones del personal interno y sus designados, incluyendo investigadores privados, de tal manera de mantener los derechos privados de la competencia. En realidad, hay una tremenda cantidad de información en

el dominio público, que si es analizada inteligentemente puede revelar una enorme información sobre la competencia.

Políticas Relacionadas:“Recopilación de Información de Precios por Terceros” e “Identidades Falsas”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

6. Distribución de los Registros del Personal

Política: Con el fin de permitir a cada empleado familiarizarse con la información y garantizar que no contenga errores, cada empleado debe recibir una copia de su archivo personal una vez al año.

Comentario: Suministrar al empleado una copia gratis de su propio archivo es una forma de reducir los reclamos sobre reportes inexactos, y una manera de garantizar que la información está actualizada y es exacta. Esta política puede ser modificada para decir, "Cada empleado debe recibir la oportunidad de obtener una copia", reduciendo así considerablemente el papeleo y gasto asociado con esta política relacionada con la integridad de la información.

Políticas Relacionadas:“Acceso a la Información Personal” y “Verificaciones de Historia Crediticia de Empleados Potenciales”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

7. Información Sobre Salud y Seguridad

Política: La gerencia debe dar a conocer plenamente a los trabajadores correspondientes, los resultados de las pruebas de sustancias tóxicas y cualquier otra información relacionada con la salud y seguridad de los trabajadores.

Comentario: Esta política está relacionada con la política del "derecho del trabajador a estar informado" sobre peligros en el sitio de trabajo. Esta política evita las demandas. Por ejemplo, en una demanda se podría alegar que el trabajador habría renunciado o se habría protegido de manera diferente si hubiese conocido esta información. Más allá de forzar a la gerencia a publicar dicha información, esta política está también dirigida a reforzar la confianza del trabajador en que la gerencia genuinamente se preocupa por el bienestar de sus trabajadores.

Políticas Relacionadas: "[Peligros Laborales](#)"

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

8. Peligros Laborales

Política: La gerencia debe informar a los trabajadores sobre la existencia de peligros en el sitio de trabajo, suministrar medidas de seguridad para minimizar el riesgo a los trabajadores y adiestrar a los trabajadores en el uso apropiado de las medidas de seguridad.

Comentario: La intención de esta política es exigir a la gerencia que dé a conocer todos los peligros. Esta política evita demandas y otras disputas y fomenta la confianza entre los trabajadores de que la gerencia se preocupa por su bienestar. Por ejemplo, si un sitio de trabajo es ruidoso, esta política requiere que la gerencia informe a los trabajadores del peligro de daño a sus oídos, suministre protectores de oídos y adiestre a los trabajadores en el uso correcto de dichos protectores.

Políticas Relacionadas: "[Información Sobre Salud y Seguridad](#)" y "[Solicitudes Externas de Información](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9. Transacciones Bursátiles de Empleados

Política: Los empleados no deben comprar o vender acciones o bonos de la Empresa X entre el fin del trimestre fiscal y el momento cuando se anuncien públicamente los resultados financieros finales.

Comentario: Esta política evita que trabajadores con acceso a información confidencial de pronta publicación, utilicen dicha información para beneficio propio en la Bolsa de Valores. El intervalo de tiempo dado es el período de tiempo en el cual podría ocurrir dicho beneficio manipulado. Después de que el público se entere de la información, hay menor ventaja especial para aquéllos con conocimiento interno. La política es relevante sólo para empresas que tienen acciones o bonos a la venta al público. Puede ser adaptada para institutos de investigación o agencias gubernamentales que recopilan y analizan información, tales como la tasa de crecimiento de la economía, cuya divulgación altera los precios de las acciones y los bonos. La política se aplica a todos los empleados, no solamente a los que trabajan en el departamento de Contabilidad, sino también a aquéllos que de alguna manera conocen los resultados financieros. La política puede ser ampliada para incluir el giro de instrucciones a terceros, tales como familiares, amigos o abogados, para comprar o vender acciones de la Empresa X en representación de los empleados o para beneficio propio. También podría ser un aditamento apropiado a la política la definición de transacción interna, pero antes se deben revisar las leyes y reglamentos locales. Serán necesarias conversaciones con un consejero legal interno sobre esta política.

Políticas Relacionadas: "[Conflictos de Intereses](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

10. Acoso Sexual, Etnico y Racial

Política: Los trabajadores no deben acosar a otros por cuestiones de sexo, etnia o raza.

Comentario: Esta política notifica a los trabajadores que el acoso no es apropiado en el trabajo y en particular en los sistemas de computación y comunicación de la Empresa X. La organización del lector puede poseer una política sobre acoso, pero esa política quizás no diga nada acerca del uso de los sistemas de la Empresa X para acosar. Las leyes sobre dicho comportamiento varían ampliamente de jurisdicción a jurisdicción, por lo que se recomienda consultar a un consejero legal. También se necesita una definición de acoso, ya que no es suficiente sólo tener una política. Se debe hacer

cumplir la política y comunicarla a los trabajadores. El alcance de esta política puede ser ampliada para incluir acoso basado en nacionalidad, edad, orientación sexual, incapacidad y creencias religiosas o políticas.

Políticas Relacionadas: “[Conducta de los Empleados Fueras de la Oficina](#)” y “[Registros de Telemercadeo](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Propiedad Intelectual Desarrollada Fuera de Sede

Política: La propiedad intelectual, incluyendo sin limitantes, patentes, derechos de autor, marcas registradas y todos los otros derechos de propiedad intelectual tal como se manifiestan en memorandos, planes, estrategias, productos, programas de computación, documentación y demás material desarrollado o concebido mientras el empleado esté trabajando en sitios alternativos de trabajo, es exclusiva propiedad de la Empresa X.

Comentario: Esta política notifica a los teletrabajadores y otros que trabajan fuera de sede que su trabajo de propiedad intelectual es propiedad de la Empresa X, a pesar de haber sido desarrollado en otra instalación. Algunas organizaciones pueden restringir esta política de tal forma que sólo haga referencia a materiales desarrollados durante las horas de trabajo o que se refieran a propiedad intelectual relacionada con el negocio de la Empresa X. La política tiene la más amplia aplicación posible, y por ende tiende a proteger a la Empresa X más que al empleado. Se recomiendan conversaciones detalladas con el consejero legal interno sobre este tópico.

Políticas Relacionadas: “[Derechos de Propiedad Intelectual](#)” y “[Derechos de Propiedad](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

12. Código de Conducta Corporativo

Política: Todos los trabajadores deben leer, entender y comportarse de acuerdo con el código de conducta corporativo.

Comentario: Esta política notifica a los trabajadores que el cumplimiento del código de conducta corporativo es obligatorio. Un código de conducta incluye mención sobre asuntos como aceptación de regalos y conflictos

de intereses. En muchos casos incluye asuntos de seguridad informática, tal como la divulgación de información sensible. En vez de ser un buen sitio para las políticas de seguridad informática, un código de conducta corporativo tiene el objeto de ser una guía para hacer negocios a la manera de la Empresa X. En un código de conducta típicamente se abordan la honestidad y otras consideraciones de alto nivel, mientras que las políticas de seguridad informática, tal como aparecen en un manual de seguridad informática o cualquier otro documento, son generalmente mucho más detalladas.

Políticas Relacionadas: “[Entendimiento del Código de Conducta](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

13. Entendimiento del Código de Conducta

Política: Todos los trabajadores deben indicar que entienden el código de conducta, firmando anualmente un formulario donde reconocen estar de acuerdo con suscribir el código.

Comentario: Esta política recuerda a los empleados que deben respetar el código de conducta de la organización. Es deseable que los empleados reconozcan por escrito que entienden que un código de conducta es requerido como parte de su trabajo. Si son despedidos como consecuencia de problemas relacionados con el código de conducta, no hay duda que los empleados entenderán qué es lo que se requería de ellos. Esta política reduce la probabilidad de una demanda por despido injustificado.

Políticas Relacionadas: “[Código de Conducta Corporativo](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

14. Conflictos de Intereses

Política: Todos los trabajadores deben evitar los conflictos de intereses, tanto los verdaderos como los aparentes, en sus tratos de negocios con la Empresa X.

Comentario: Esta política informa a los trabajadores que no es suficiente no tener conflictos de intereses. Tampoco debe haber apariencia de conflicto de intereses. Por ejemplo, un gerente puede ser dueño de un bloque de acciones de una compañía de la competencia a través de un fideicomiso. Aunque el

gerente no tenga influencia sobre la compañía competidora, y pueda no tener relaciones especiales o acceso a la información de la compañía competidora, la propiedad de las acciones por parte del gerente implica un conflicto de intereses. Si el hecho de ser el dueño de esas acciones llegara a los periódicos, o si clientes importantes se enteran de esto, se dañaría la reputación del gerente y la de la Empresa X. Mucha organizaciones querrán suplementar esta política con ejemplos, tales como tener un pariente cercano trabajando para la competencia. Más que cualquier otra política de este manual, es posible que esta política se integre al Código de Conducta.

Políticas Relacionadas: “Transacciones Bursátiles de Empleados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Relaciones Personales con la Competencia

Política: Los trabajadores de la Empresa X no deben tener compañeros románticos o familiares cercanos trabajando en organizaciones de la competencia.

Comentario: Esta política evita la divulgación involuntaria de información confidencial. Hasta un comentario informal puede transmitir información que pudiera ser usada por un competidor. Esta política sirve también como protección contra el espionaje industrial o militar donde un(a) compañero(a) romántico(a) es también un(a) espía. El alcance de esta política puede ser restringido a aquéllos que trabajan en el departamento de Investigación y Desarrollo, o cualquier otra actividad particularmente sensible.

Políticas Relacionadas: “Compartir Información de Mercadeo” y “Acuerdos de Confidencialidad con Antiguos Patronos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

16. Renuncia de Empleados por la Competencia

Política: Todos los trabajadores que tengan la intención de trabajar para un competidor deben notificar inmediatamente a la gerencia de la Empresa X y, al momento de aceptar la oferta del competidor, el trabajador recogerá sus pertenencias personales en presencia de un escolta

quien lo acompañará hasta la puerta, revocándose entonces todos sus derechos, privilegios y accesos a la Empresa X.

Comentario: La intención de esta política es que quede claro que cualquier empleado que próximamente se va a trabajar para la competencia, no debe permanecer en las instalaciones de la Empresa X y no debe permanecer como usuario autorizado de los sistemas informáticos. Esto es cierto sin importar el tipo de cese de que se trate, sea éste despido justificado o no, renuncia o jubilación. El acceso a cualquier sistema es una oportunidad para los empleados salientes de tomar listas de dirección de correo y otra información que pudiese ser de utilidad al nuevo empleador. Una de las cosas más eficaces que una organización puede hacer para manejar estas situaciones es establecer una política despidiendo a todos los trabajadores que anuncian que se van a trabajar con la competencia. Esta política también envía un mensaje a todo el personal remanente de que el ex-empleado ya no es un integrante del grupo de confianza. La existencia de una política como ésta hace aceptable desde los puntos de visto diplomático y social lidiar decisivamente con este tipo de trabajador que se va. Esta política es una manifestación especial de la noción de conflicto de intereses. Esta política es adecuada para aquellas organizaciones que tienen una alta rotación de personal, tal como las organizaciones de alta tecnología.

Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia” y “Eliminación de Archivos de Trabajador Cesado”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

17. Notificación de Cese de Empleo

Política: Todos los empleados deben ser informados tan pronto se produzca el cese de un empleado, y el departamento de Recursos Humanos debe frecuentemente recordar a los empleados que los ex-trabajadores no deben entrar a las instalaciones de la Empresa X, usar los recursos de la Empresa X o estar afiliados de ninguna forma a la Empresa X.

Comentario: Esta política consigue el apoyo y participación de los empleados restantes para asegurar la separación entre internos y externos. Si los trabajadores restantes van a actuar como un sistema de aviso temprano, ellos deben ser informados que ciertos ex-trabajadores no deben entrar en los edificios de la Empresa X, en los computadores de la Empresa X y no

deben tener ningún tipo de conexión con la Empresa X. Esta política va muy bien con una política de atención que requiere que los trabajadores restantes soliciten saber, de todas las personas que se encuentren dentro de las áreas restringidas y que no llevan una ficha con foto, quiénes son y por qué están allí. Esta política tiene un alcance más amplio de notificación que la efectuada por muchas organizaciones, donde sólo los administradores de sistemas y otros responsables por actualizar los controles de acceso a computadores reciben tal notificación. Esta política deliberadamente no hace distinción entre ceses laborales voluntarios e involuntarios. Tal notificación se hace fácilmente mediante correo electrónico, y si existen fotos de los trabajadores en la red interna, esta política será más efectiva debido a que la persona puede ser fácilmente reconocida.

Políticas Relacionadas: “[Escolta para Trabajadores Despedidos](#)” e “[Informe de Cambios en Situación de Empleados](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

18. Notificación a Terceros de Cese de Trabajador

Política: Si un trabajador despedido tiene la autoridad de dirigir contratistas, consultores o temporales, o si este mismo trabajador tiene la autoridad para comprometer a la Empresa X en una compra u otra transacción, entonces el departamento de Recursos Humanos debe notificar inmediatamente a todos los terceros pertinentes que el trabajador despedido ya no es empleado de la Empresa X.

Comentario: Esta política evita que trabajadores despedidos se dirijan a terceros en forma alguna. Un trabajador despedido puede tener espíritu de venganza y puede obligar a la Empresa X a la compra de algunos bienes o puede comprometer a la Empresa X en otra transacción o contrato. Un ex-empleado también puede avergonzar a su ex-empleado actuando de manera no profesional, quizás ofreciendo vender cierta información confidencial. Si terceras partes piensan que el ex-empleado es empleado de la Empresa X, tendrá más credibilidad. Esta es una razón para retirar las tarjetas de presentación, tarjetas de crédito y cualquier otra evidencia de afiliación al momento del cese. Un ex-empleado también podría utilizar la confianza generada por el empleo para hacer ingeniería social y así obtener claves y otros códigos de acceso a sistemas que

pueda utilizar para entrar en los computadores del ex-empleado. Esta política aclara la distinción entre trabajadores actuales y ex-empleados. El acto de notificar a los terceros puede también traer a la luz ciertas irregularidades que posiblemente no habían sido oficialmente detectadas anteriormente. Por ejemplo, si un descuento especial y no autorizado estaba siendo otorgado a un distribuidor, este distribuidor podría preguntar si el descuento seguirá disponible. Algunas organizaciones logran el mismo resultado cuando el reemplazo del trabajador hace contacto con cada contratista, consultor, temporal o vendedor importante para informarles que el ex-empleado ya no está autorizado para ciertas actividades.

Políticas Relacionadas: “[Acceso Físico de Trabajadores Cesados](#)” y “[Responsabilidad por Cese de Trabajador](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

19. Manejo de Despidos

Política: En todos los casos cuando trabajadores de apoyo técnico de tecnología informática sean despedidos, inmediatamente deben ser relevados de sus cargos, exigirles la devolución de todo el equipo e información de la Empresa X y escoltarlos mientras empacan sus pertenencias y salen de las instalaciones de la Empresa X.

Comentario: Debido a que los trabajadores de tecnología informática pueden causar daños considerables, es prudente eliminar inmediatamente la posibilidad de que puedan tomar represalias contra su ex-patrono como venganza. Esta política se refiere específicamente a los trabajadores de apoyo técnico ya que ellos están en una posición importante de confianza. Nótese que la política sólo menciona a aquéllos que tienen suficientes privilegios especiales como para tener un efecto sobre lo que hacen los usuarios finales. Al respecto, se hace una distinción entre los trabajadores de apoyo técnico a la tecnología informática y los trabajadores de tecnología informática. Palabras adicionales referentes a la revocación inmediata de privilegios en el sistema representan también una posible ampliación de esta política.

Políticas Relacionadas: “[Despidos Inmediatos](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

20. Escolta para Trabajadores Despedidos

Política: En todos los casos cuando los trabajadores sean despedidos por la Empresa X, la finalización del servicio debe ser efectuada en presencia de un guardia de seguridad, y seguidamente el despedido debe empacar sus pertenencias también en presencia del guardia de seguridad, ser escoltado a la puerta y ser informado que no puede volver a entrar a las instalaciones a menos que sea invitado por la gerencia.

Comentario: Esta política evita actos de venganza, especialmente daños a la información computarizada. Una vez que los trabajadores son despedidos, no deberán tener ningún tipo de acceso a los registros computarizados de la Empresa X. Si los trabajadores tienen información personal en los sistemas informáticos de la Empresa X y existe una política en contra del uso personal, entonces dicha información puede ser abandonada porque es evidencia de violación de esa política. Si no existe una política de uso personal, un supervisor puede retirar la información personal y enviarla al trabajador en un disquete o medio similar de almacenamiento. Los privilegios de acceso al sistema del trabajador deben ser revocados antes de emitirse la notificación formal de su despido. Esta política asume que hay otro proceso para la recopilación de tarjetas telefónicas, tarjetas de crédito, celulares, llaves de oficina, fichas de identificación y artículos similares. La política también asume que la organización tiene guardias de seguridad.

Políticas Relacionadas: “Despidos Inmediatos” y “Responsabilidad por Cese de Trabajador”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

21. Retención de Información al Terminar Empleo

Política: Toda la información de la Empresa X en custodia del trabajador saliente, debe ser entregada a su supervisor inmediato al momento de su salida, con la excepción de copias personales de información diseminadas al público y copias personales de correspondencia directamente relacionadas a los términos y condiciones del empleo.

Comentario: Esta política establece que la información interna de la Empresa X no debe quedar en posesión del trabajador cuando éste se va de la Empresa X. Con mucha frecuencia los trabajadores se llevan todo tipo de información pensando que los ayudará en sus próximos empleos. La política implica que los trabajadores no

deben tratar de negociar el suministro de la información con su supervisor cuando se retiren. Las palabras "de forma legible" pueden añadirse para enfatizar que la información entregada al supervisor inmediato del trabajador debe ser accesible y no cifrada. Idealmente, esta política es utilizada conjuntamente con una política que diga que la Empresa X es propietaria de toda la información creada por los trabajadores durante el transcurso del empleo, excepto cuando existan convenios escritos que incluyan arreglos diferentes. Algunas organizaciones generalizan esta política para incluir contratistas, consultores, temporales y otros tipos de trabajadores, además de los trabajadores formales.

Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

22. Devolución de Propiedad al Cesar Empleo

Política: En el momento que cualquier empleado, consultor o contratista termine su relación con la Empresa X, toda propiedad de la Empresa X debe ser devuelta, incluyendo, sin limitantes, computadores portátiles, libros de la biblioteca, documentación, llaves del edificio, tarjetas magnéticas de acceso, tarjetas de crédito y préstamos pendientes.

Comentario: Esta política señala que se debe recuperar toda propiedad de la Empresa X antes de que el empleado abandone las instalaciones e, idealmente, antes de entregarle su cheque de pago final. Si las propiedades de la Empresa X no son recuperadas en ese momento, será sumamente difícil recolectarlas después. Se presentan problemas cuando pertenencias de la Empresa X se encuentran en la residencia del trabajador, en su vehículo, o en otros sitios que no están bajo el control directo de la Empresa X y, en estos casos, durante el último día de trabajo del trabajador, la Empresa X deberá obtener del trabajador una constancia por escrito de que tiene en su poder propiedad de la empresa, acompañada de la promesa de devolverlo. Si el ex-empleado se va a quedar con un computador de la empresa, representantes de la Empresa X deben examinar el disco duro para asegurarse que no contiene información confidencial. Esta política sólo sugiere una lista de propiedades que deben ser devueltas. Cada organización deberá elaborar su propia lista dependiendo de la naturaleza del negocio y las herramientas que utilicen. Esta lista por lo general no se especifica en la política pero sí en una lista aparte de verificación para la gerencia, al momento de finalizar la

relación de trabajo, y es mejor hacer que la política haga referencia a la lista en vez de utilizar la política tal como está actualmente.

Políticas Relacionadas:“Responsabilidad por Cese de Trabajador” y “Acceso Físico de Trabajadores Cesados”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

23. Días Consecutivos de Vacaciones

Política: La gerencia debe garantizar que los trabajadores saldrán de vacaciones por lo menos cinco días consecutivos una vez al año.

Comentario:Esta política evita que los trabajadores oculten un fraude u otros actos abusivos o ilegales. Si los trabajadores vienen a trabajar todos los días laborables, tendrán más oportunidad para esconder estas actividades. Un período vacacional de cinco días laborales es suficiente para que otro trabajador se involucre en las actividades propias de la persona que está de vacaciones. Cuando alguien diferente se involucra, es muy probable que esa persona se dé cuenta de irregularidades. Cuando una persona adicional realiza cierta tarea, entonces ocurre cierta cantidad de adiestramiento cruzado. Esta política también sirve como un detector de abusos y fraudes que están ocurriendo. Otro beneficio de esta política es que requiere que los empleados tomen vacaciones, lo cual puede evitar significativas acumulaciones de vacaciones que a la larga constituirían una obligación mayor para las finanzas de la organización. La política también ayuda a que los trabajadores adictos al trabajo tomen vacaciones que normalmente no quieren tomar. Esta política pudiera ser un anexo a una política que obligue a los trabajadores a tomar sus vacaciones o correr el riesgo de perderlas.

Políticas Relacionadas:“Adiestramiento Multidisciplinario”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

24. Segundos Trabajos

Política: Los trabajadores no deben tener un segundo trabajo si el mismo perjudica o compromete de alguna manera la objetividad del trabajador en su cargo con la Empresa X, o si el otro patrono está de alguna manera en competencia con la Empresa X.

Comentario:Muchas personas sienten presión económica y toman un segundo trabajo. Esta política intenta garantizar que estos segundos trabajos no conlleven problemas de seguridad informática para la Empresa X. Por ejemplo, si un agente de compras toma un segundo trabajo con quien vende a la Empresa X, se comprometería su habilidad para efectuar objetivamente las labores de compras y sería suficiente para terminar su relación de trabajo. Este tipo de trabajos secundarios involucra pagos no contabilizables al empleado de la Empresa X por desviar negocios hacia el vendedor. Estos pagos pueden ser no detectados sin una política como ésta y sin el monitoreo de los segundos trabajos del empleado. Igualmente, si un trabajador acepta un trabajo con un competidor, puede haber cierta presión para robar información propiedad del primer empleador. La política puede ampliarse con palabras que digan que "si hay alguna duda sobre la interpretación de estas palabras, consulte al gerente o al departamento de Recursos Humanos". Como otro punto, la política debería aplicarse a trabajos de consultoría, asignaciones como contratista y posiciones temporales, no sólo a los trabajos tradicionales de tiempo completo y permanente.

Políticas Relacionadas:“Divulgación de Segundos Trabajos,” “Conflictos de Intereses,” y “Días Consecutivos de Vacaciones”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

25. Divulgación de Segundos Trabajos

Política: Los trabajadores deben informar a su gerente inmediato que tienen un segundo o más trabajos en el momento en que son entrevistados para optar por una posición en la Empresa X o, si ya están empleados en la Empresa X, al momento de tomar estos otros trabajos.

Comentario:Esta política garantiza que la gerencia estará informada de los segundos o terceros empleos que el personal de la Empresa X desempeña actualmente. Esto ayudará a la gerencia a entender las variaciones en el desenvolvimiento del trabajador, posiblemente debido a falta de descanso y también a determinar si existe un conflicto de intereses o si el otro trabajo compromete la objetividad del trabajador de alguna forma mientras ejecuta sus labores para la Empresa X. La política puede adicionalmente ayudar a detectar problemas potenciales de relaciones públicas o legales tal como directores simultáneos de compañías grandes e influyentes. La información prevista en esta política puede ser de más utilidad cuando se investigan fraudes potenciales u otros problemas que involucren a

múltiples organizaciones. La política es un mecanismo para asegurarse de que la gerencia tiene una buena idea de las intenciones que promueven el comportamiento del trabajador.

Políticas Relacionadas: "Segundos Trabajos," "Renuncia de Empleados por la Competencia," y "Días Consecutivos de Vacaciones"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

26. Trabajadores Como Clientes

Política: Los trabajadores de confianza actualmente en posiciones relacionadas con computación en la Empresa X no deben ser al propio tiempo clientes de la Empresa X.

Comentario: Esta política evita las tentaciones e impide una variedad de abusos que se fomentan, dado que los trabajadores tienen privilegios de acceso a los sistemas informáticos de la Empresa X. Por ejemplo, si un oficinista que ejecuta transferencias de giros en un banco tuviese una cuenta en el mismo banco, podría facilitar transferencias fraudulentas. Esta política reduce la sospecha sobre trabajadores en posiciones de confianza relacionadas con computación. La política está dirigida primordialmente a esas organizaciones que tratan con tipos de información valiosa, especialmente aquéllas con dinero computarizado. Por ejemplo, una cadena de supermercados probablemente no adoptaría una política como ésta. La política también puede ser de utilidad donde la separación de labores es inadecuada. Si se adopta esta política, se debe definir el criterio para determinar si la posición es de confianza en lo relativo a computación. Este criterio puede incluir la habilidad de causar daños relacionados con computación a la Empresa X por encima de los \$100.000, la habilidad de modificar los archivos de los sistemas de producción de tal manera que la actividad fraudulenta se pueda esconder fácilmente, o la habilidad de alterar los registros de los clientes de manera anónima.

Políticas Relacionadas: "Fianzas de Trabajadores" y "Trabajo en Proyectos Sensibles"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Altos

27. Informe de Cambios en Situación

Política: Los empleados deben reportar a su gerente inmediato todos los cambios en su situación personal que pudiesen afectar su elegibilidad para mantener su cargo actual o, de lo contrario, estarán sujetos a acciones disciplinarias que podrían incluir la finalización de la relación de trabajo.

Comentario: Esta política extiende el tiempo otorgado a los empleados para informar sobre su situación personal, más allá del momento en el cual se toma la decisión de emplearlos. En la mayoría de las organizaciones generalmente no hay una política obligatoria de divulgación, una vez empleada la persona. Cambios en la situación del empleado afectan el grado de confianza que la gerencia le tiene para permitir su acceso a información sensible y otros activos, tales como dinero efectivo. Los trabajadores de computación están en una posición de confianza de alto poder, que puede ser explotada en detrimento del patrono. Esta política evita tales situaciones difíciles.

Políticas Relacionadas: "Revisión de Antecedentes"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

28. Transferencias de Trabajadores

Política: Los trabajadores que hayan declarado su intención de abandonar el empleo en la Empresa X y aquéllos que estén en conocimiento de su inminente despido y cualquier empleado descontento, deben ser transferidos a posiciones donde sólo puedan hacer mínimo daño a los activos de la Empresa X.

Comentario: Esta política evita que los empleados disgustados o descontentos puedan seguir en una posición donde causen serios daños a la propiedad de la organización, incluyendo la información manejada por los sistemas de computación y comunicación. Por ejemplo, el mantener a un programador de sistemas en su trabajo después de haber sido notificado de su despido, es una invitación a problemas. La política no hace referencia específica a trabajadores relacionados con computadores y comunicaciones, porque la política se debería aplicar a todos los trabajadores. Por ejemplo, un guardia de seguridad de la entrada del edificio que haya entregado su preaviso debería, de acuerdo con esta política, ser removido de su puesto. La política ha sido deliberadamente redactada de tal forma que requiere que la gerencia use su discreción. En algunas organizaciones, un guardia de seguridad pudiera estar en una

posición para hacerle daño a los activos de la organización, mientras que en otras organizaciones, un guardia de seguridad no podría hacer mucho daño.

Políticas Relacionadas: “Acceso Físico de Trabajadores Cesados” y “Confidencialidad de la Información de las Investigaciones Internas”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

29. Resolución de Quejas

Política: La gerencia debe establecer y suministrar personal adecuado para realizar los procedimientos que agilicen todas y cada una de las quejas del trabajador.

Comentario: Esta política comunica a los gerentes de bajo nivel el requerimiento para la pronta solución de las quejas del trabajador. Nótese que la política no requiere que las quejas sean resueltas de una manera satisfactoria para los trabajadores, sólo que cada una sea atendida prontamente. Contar con un proceso de resolución de quejas levanta la moral de los empleados, haciéndoles saber que la gerencia sí se interesa por lo que tienen que decir. Esta política también es consistente con el compromiso de que la calidad es parte de todos los procesos del negocio. Algunas quejas pueden estar relacionadas con deficiencias en el control y las quejas pueden suministrar valiosa información para mejorar el control interno. La pronta solución de las quejas también minimiza el riesgo de un delito informático u otro abuso, en caso de que el trabajador sienta la necesidad de vengarse o de alguna manera hacerse sentir. En algunas organizaciones se establece un mediador como juez imparcial a quien se llevarán las quejas no resueltas.

Políticas Relacionadas: “Negativa a Proporcionar Información Inneccesaria”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

30. Orientación Confidencial

Política: Todo trabajador con serios problemas personales deben recibir asesoramiento confidencial y gratuito.

Comentario: Esta política ayuda a los trabajadores en la resolución de problemas personales de tal manera que sus problemas no interfieran en demasía con su capacidad para realizar el trabajo. Por ejemplo, si un

trabajador fuese un adicto a las drogas, podría verse afectada su habilidad de razonamiento y crear un problema. Si un trabajador estuviera bajo una severa presión económica, pudiera estar tentado a vender información confidencial a la competencia. Muchas organizaciones proveen algún tipo de asesoramiento como parte de un plan de seguros médico. Sin embargo, en algunos casos es mejor dejar fuera de la política la duración y naturaleza del asesoramiento de un servicio específico. Esto le da a la gerencia la posibilidad de cambiar los servicios ofrecidos dentro los planes de seguros de salud, a medida que cambian los beneficios conexos. Aunque poco frecuente, la política también puede establecer límites en el número de visitas al consejero, el costo total o el tiempo que duran los servicios gratuitos. Los arreglos de pagos compartidos, cuando el trabajador paga parte de los costos, son también comunes, aunque esto se menciona en otra parte. Por razones similares se recomienda a las organizaciones considerar préstamos libres de interés para aquellos trabajadores que se encuentran en necesidad de dinero extra urgentemente.

Políticas Relacionadas: “Drogas y Alcohol” y “Resolución de Quejas”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

31. Drogas y Alcohol

Política: Con excepción de las medicinas recetadas por un profesional médico, los trabajadores no deben usar o estar bajo la influencia de drogas o de alcohol en el sitio de trabajo.

Comentario: Esta política estimula a los trabajadores a estar sobrios en el sitio del trabajo, ya que de esta manera están en mejor capacidad de tomar decisiones racionales y mantenerse dentro de los objetivos de la organización. Algunas organizaciones pueden establecer una política escrita en caso de tener que disciplinar a un trabajador o despedirlo debido al uso de drogas o alcohol en el trabajo. Para los trabajadores que realizan el trabajo fuera de las instalaciones de la empresa, incluyendo vendedores que trabajan en sus vehículos, la ubicación del sitio de trabajo no es tan clara como solía ser. En una organización virtual, el sitio de trabajo está donde la gente hace su trabajo. Esta política puede causar problemas con algunos empleados que ingieren licor en su hora de almuerzo, particularmente si están acompañados de posibles clientes. Ejerciendo un buen juicio en estas raras ocasiones sería suficiente, lo cual eliminaría la necesidad de una

mención específica de estos hechos en la política. Para ejercer una política como ésta, un pequeño pero creciente número de organizaciones están utilizando exámenes de sobriedad computarizados, los cuales consisten en juegos de video que examinan los reflejos del trabajador para asegurarse de que está sobrio antes de comenzar su trabajo.

Políticas Relacionadas: “Orientación Confidencial”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

32. Remoción de Distintivos de Identificación

Política: Inmediatamente después de salir del área de la Empresa X, los trabajadores deben quitarse el distintivo de identificación y guardarlo en un lugar seguro y conveniente fuera de la vista pública.

Comentario: Esta política evita que los trabajadores salgan de su sitio de trabajo con el distintivo de identificación, indicándole indirectamente a todo el mundo que ellos trabajan para la Empresa X. Mantener el distintivo de identificación en público hace que los espías corporativos o hackers intenten obtener información de ese trabajador. Esta política es especialmente importante para aquellas organizaciones que desean que su personal se mantenga anónimo. Esta política adicionalmente fomenta la colocación correcta del distintivo y cómo su colocación se corresponde con la ubicación física del trabajador.

Políticas Relacionadas: “Acceso Físico para Terceros” y “Escolta para Trabajadores Despedidos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

33. Aseguramiento de los Distintivos

Política: Al estar fuera del área de la Empresa X, los trabajadores deben proteger su distintivo de identificación de la misma manera que protegen sus carteras o tarjetas de crédito.

Comentario: Esta política enfatiza que los distintivos de identificación de la Empresa X son valiosos y que, por lo tanto, necesitan tanta protección como la billetera. Además, se espera que los empleados protejan sus distintivos del robo o uso no autorizado. En muchas ocasiones, los trabajadores dejan sus distintivos en un carro abierto o en otros lugares claramente visibles de donde pueden ser robados fácilmente. Un intruso que intenta entrar en las instalaciones de la Empresa X quiere obtener un distintivo para analizar sus componentes y poder así determinar cómo hacer una falsificación. Si el intruso no puede obtener un distintivo existente, el proceso de falsificación será mucho más difícil. Si la tecnología utilizada para el distintivo no es sofisticada, el intruso puede remover la foto existente e insertar su propia imagen en el distintivo. Esta política es deliberadamente neutra sobre la tecnología y ni siquiera requiere que se utilice una foto en el sistema de distintivos de identificación de la organización.

Políticas Relacionadas: “Personas Sin Distintivos de Identificación” y “Acceso Físico para Terceros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

6.02 Adiestramiento de Usuarios

6.02.01 Educación y Adiestramiento en Seguridad Informática

1. Exámenes Sobre las Políticas

Política: Los usuarios no deben tener acceso a los sistemas informáticos de la Empresa X, a menos que hayan leído la Política de Seguridad Informática y tomado un pequeño examen que demuestre claramente que entienden el material descrito en dicha política.

Comentario: Uno de los mayores problemas con las políticas de seguridad informática gira en torno a saber si los usuarios han leído y entendido las políticas. Si los usuarios no han leído las políticas, por desconocimiento

pueden hacer cosas que causen problemas de seguridad; por ejemplo, abrir un archivo enviado como adjunto a un correo electrónico sin haber examinado el archivo con un paquete antivirus. Si los usuarios han leído las políticas, pero no las han entendido suficientemente, pueden hacer cosas que causen problemas de seguridad. La verdadera prueba del entendimiento sería observarlos trabajando en su ambiente de trabajo, pero eso es muy costoso para casi todas las organizaciones. Lo más recomendable es hacerles tomar un pequeño examen para determinar si han entendido la política. Si pasan el

examen, se les puede otorgar el privilegio de acceso. Por ejemplo, un trabajador que desea trabajar desde su casa puede leer la política de seguridad para estos casos, presentar un examen y aprobarlo, y en ese momento el administrador de seguridad autorizará al usuario a acceder a la red interna de la organización a través de Internet utilizando una red privada virtual. En organizaciones sofisticadas, tales privilegios se abren automáticamente, basándose en un examen entregado a través de un software de adiestramiento asistido por computador desde la intranet.

Políticas Relacionadas: “[Formularios para Identificadores de Usuario](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Políticas y Procedimientos Relativos a la Privacidad

Política: Con excepción de los relativos al manejo de datos privados de las personas, las políticas y procedimientos de seguridad informática deben ser revelados sólo a los trabajadores de la Empresa X y a terceros seleccionados, tales como los auditores, quienes tienen una necesidad legítima de negocio sobre esta información.

Comentario: Esta política tiene que ver con la política aparentemente contradictoria que establece que la información sobre seguridad debe ser restringida solamente a los internos, pero puede ser revelada a los externos. Algunas organizaciones pueden querer ir un paso más allá, añadiéndole una oración al final de la política que indique que la Empresa X reconoce que las personas tienen intereses personales en la información sobre sí mismos. Esta política es bastante progresiva y refleja las políticas de privacidad actualmente en uso en varias compañías de teléfonos y agencias gubernamentales. Las prácticas comunes en diferentes tipos de negocios en el mundo entero pueden variar. La política es deliberadamente vaga sobre la información específica que será divulgada, dejando la decisión a la gerencia. Un esquema de clasificación de datos debe usarse para designar cuál información es pública.

Políticas Relacionadas: “[Anonimato del Cliente](#)” y “[Reportes Externos de Violaciones](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Adiestramiento para Acceso Remoto

Política: Los trabajadores de la Empresa X deben completar y aprobar un curso de adiestramiento de acceso remoto a los sistemas, antes de recibir el privilegio de acceso a una red conmutada, a los protocolos que permiten la conexión e introducción de comandos en un computador remoto conectado a Internet, o cualquier otro acceso remoto al sistema de comunicación de datos.

Comentario: Al reconocer los problemas de seguridad asociados con el sistema de teletrabajo y otros tipos de sistema de acceso remotos, esta política insiste que todos los usuarios de las facilidades de acceso remoto a la Empresa X deben estar adecuadamente adiestrados. El curso de adiestramiento mencionado en esta política incluye temas de seguridad, tales como proteger de robo los equipos ubicados en lugares remotos, el cifrado de archivos sensibles almacenados en el disco duro de un computador remoto, hacer trizas las copias impresas antes de desecharlas, guardar las copias impresas en gabinetes o contenedores seguros similares y los pasos requeridos en seguridad para establecer una conexión al sistema de comunicación de datos.

Políticas Relacionadas: “[Requisitos de Seguridad para Teletrabajo](#)” y “[Procedimientos de Seguridad Informática en Teletrabajo](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Adiestramiento en Internet

Política: Los trabajadores pueden acceder a Internet a través de los servicios de la Empresa X sólo si han sido autorizados por la gerencia del departamento y han completado un curso de adiestramiento en políticas y prácticas de Internet.

Comentario: Esta política evita el uso ilimitado de Internet por los trabajadores de la Empresa X. Debido a que el uso de Internet presenta una cantidad de problemas serios de seguridad, es apropiado un curso separado de adiestramiento. Preferiblemente el curso de adiestramiento se haría a través de un computador, lo que permitiría a los usuarios completar el adiestramiento a su conveniencia. La política no prohíbe a la gerencia establecer requerimientos adicionales para otorgar los permisos de acceso a Internet. Estos requerimientos pueden incluir la necesidad de acceso por asuntos del negocio.

Políticas Relacionadas: “Adiestramiento en Seguridad Informática” y “Tiempo de Adiestramiento”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

5. Panfleto sobre Políticas de Seguridad Informática

Política: Antes o en su primer día de trabajo, todos los nuevos trabajadores de la Empresa X deben recibir una copia del folleto informativo de la política de seguridad informática y hacerles saber que deben satisfacer los requisitos descritos en el folleto.

Comentario: Esta política garantiza que todos los nuevos trabajadores conocen las reglas de seguridad informática, las han leído y entienden que deben cumplirlas. En estos días muchas organizaciones no distribuyen un manual completo de seguridad informática, prefiriendo a cambio suministrar un folleto breve que contiene los puntos más resaltantes. Estos folletos típicamente contienen una dirección de intranet en donde está ubicada toda la información sobre políticas, normas, procedimientos y responsabilidades de seguridad informática. Este procedimiento permite que los requerimientos de seguridad informática sean actualizados rápida y automáticamente sin necesidad de distribuir nuevos manuales impresos a todos los trabajadores. A cambio, una nota de correo electrónico puede ser enviada a todas las personas que deben seguir estos requerimientos. Entregar a los nuevos trabajadores un folleto con su nuevo paquete de materiales, enfatiza el compromiso de la gerencia con la seguridad informática y les hace prestar atención a ello desde el principio de su relación de empleo.

Políticas Relacionadas: “Entendimiento del Código de Conducta” y “Adiestramiento en Seguridad Informática”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Adiestramiento en Seguridad Informática

Política: Todos los trabajadores deben ser provistos con suficiente adiestramiento y material de referencia de soporte para permitirles proteger adecuadamente los recursos informáticos de la Empresa X.

Comentario: Esta política requiere que aquellos trabajadores que manejan la información de la Empresa X sean dotados de suficiente adiestramiento y documentación

en seguridad informática. El material específico que debe ser entregado a los trabajadores puede variar basado en la naturaleza del trabajo que ejecuten. Por ejemplo, las telefonistas que reciben órdenes por teléfono deben recibir un adiestramiento diferente del que reciben los programadores de computadores. En muchas organizaciones, casi todos los trabajadores tienen acceso a la información de la Empresa X para poder ejecutar su trabajo. Sin embargo, muchos trabajadores necesitan sólo un adiestramiento rudimentario. La política comunica desde la alta gerencia hasta la baja gerencia los requerimientos para el adiestramiento y la documentación, los cuales pueden estar en línea en lugar de estar impresos. Esta política descansa en la decisión de la gerencia local con respecto a qué constituye suficiente adiestramiento en seguridad informática. Algunas organizaciones pueden preferir decir que el departamento de Seguridad Informática determina lo que constituye suficiente adiestramiento.

Políticas Relacionadas: “Tiempo de Adiestramiento,” “Manual de Seguridad Informática,” “Responsabilidades del Usuario de la Información,” y “Adiestramiento Técnico y Educación Continua”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

7. Adiestramiento Básico

Política: Los trabajadores deben haber terminado satisfactoriamente todos los otros adiestramientos básicos necesarios para efectuar su nuevo trabajo antes de recibir el adiestramiento de seguridad informática.

Comentario: Esta política evita que algunas personas tomen el curso de adiestramiento de seguridad informática sin antes pasar los otros cursos de adiestramiento. La tardanza en adiestramiento que se menciona en esta política, también le dará a muchas organizaciones tiempo adicional para completar la verificación de antecedentes de los nuevos empleados, si es que no han sido completados. La política evitará que gente incompetente obtengan acceso a información que pueda ser utilizada para comprometer la seguridad informática en la Empresa X. Considérese el modelo actual en muchos bancos. Los cajeros no reciben adiestramiento de seguridad hasta tanto no pasan otros adiestramientos y hasta que demuestran que pueden manejar cualquier actividad que requiera el trabajo. En un sentido esta política restringe la información sobre seguridad a aquéllos que la necesitan y en ese aspecto es una manifestación del concepto general conocido como la necesidad de conocer. Nada de lo mencionado en esta

política insinúa que los nuevos trabajadores deben ser colocados en sus puestos de trabajo antes de recibir adiestramiento en seguridad informática.

Políticas Relacionadas: “Adiestramiento para Acceso Remoto” y “Comandos y Capacidades del Sistema”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

8. Cambios en Políticas de Seguridad Informática

Política: Todos los trabajadores de la Empresa X deben recibir notificación pronta de los cambios realizados a la política de seguridad informática de la empresa, incluyendo la manera en que estos cambios pueden afectarlos y cómo obtener información adicional.

Comentario: Esta política garantiza que todos los trabajadores estarán enterados de la última versión de la política de seguridad informática. Sin una política como ésta, puede haber problemas legales asociados con disciplina y despidos que se basaron en una política de seguridad informática que no había sido comunicada a los trabajadores involucrados. Estos trabajadores pueden decir que no pueden razonablemente ser responsables de una norma o comportamiento definido en una política sobre la cual no han sido informados debidamente. Esta política claramente establece la intención de la gerencia de informar a todos los trabajadores involucrados, a pesar de que no especifica cómo se les informará. Esto variaría de acuerdo al grupo receptor y los sistemas informáticos disponibles. El correo electrónico es una de las vías más económicas y el correo electrónico puede contener una dirección de intranet donde se pueden encontrar todos los detalles. También es efectivo una nota adjunta a su cheque o sobre de pago.

Políticas Relacionadas: “Aviso de Cambio en Política de Privacidad” y “Entendimiento del Código de Conducta”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

9. Responsabilidad en Adiestramiento

Política: El departamento de Seguridad Informática debe proporcionar cursos de actualización y otros materiales, para recordar regularmente a los trabajadores sus obligaciones con respecto a la seguridad informática.

Comentario: Esta política define quién tiene la responsabilidad de suministrar adiestramiento en seguridad informática, su documentación y material relacionados. Esta responsabilidad puede no estar adecuadamente asignada y entonces algunos trabajos importantes de seguridad informática terminan por no hacerse. También se pueden agregar a la política otros departamentos, además de Seguridad Informática. Otro objetivo de la política es subrayar el hecho de que el adiestramiento y la toma de conciencia no es un esfuerzo que se hace una sola vez. Este tipo de trabajo necesita que se haga periódicamente. Entre líneas está escrita en esta política la admisión por parte de gerentes de departamentos y otros niveles inferiores, que deben dar a sus trabajadores suficiente tiempo para asistir a cursos de actualización, manejar programas de software y leer la documentación, entre otras actividades. La política utiliza la palabra “trabajadores”, con la intención de cubrir a todas las personas que pudieran estar en una posición donde necesitarían conocer los recursos adecuados para proteger la información de la Empresa X.

Políticas Relacionadas: “Tiempo de Adiestramiento” y “Tareas del Departamento de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Tiempo de Adiestramiento

Política: La gerencia debe asignar tiempo hábil para que los trabajadores se familiaricen con las políticas de seguridad, procedimientos y otras formas de llevar los negocios en la Empresa X.

Comentario: No es realista suponer que los empleados leerán los materiales de seguridad de informática durante su tiempo libre. No sólo se requiere este adiestramiento sino que la gerencia debe dar a sus empleados suficiente tiempo para familiarizarse con los materiales. Algunos gerentes consideran que no vale la pena utilizar el tiempo del trabajador en la seguridad informática, ya que ello no contribuye directamente a las ganancias.

Políticas Relacionadas: “Adiestramiento en Sistemas de Producción” y “Responsabilidad en Adiestramiento”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

11. Convenio de Trabajo

Política: Todo trabajador debe entender las políticas y procedimientos de la Empresa X referentes a seguridad informática y debe estar de acuerdo, por escrito, en ejecutar su trabajo de conformidad con dichas políticas y procedimientos.

Comentario: Esta política requiere que cada trabajador se familiarice con las políticas y procedimientos de seguridad informática, pero también busca confirmar por escrito que entiende y está de acuerdo en firmar una declaración mediante la cual acepta estar obligado a seguir dichas políticas y procedimientos. Desde un punto de vista legal, es deseable que los empleados confirmen por escrito que entienden que la seguridad informática es parte de su trabajo. Si son despedidos debido a una violación de la seguridad informática o problemas relacionados, no habrá duda alguna que tales empleados entendieron lo que se requería de ellos. Por lo tanto esta política reduce la probabilidad de una demanda de despido injustificado. El obtener algo por escrito también brinda una nueva credibilidad a algo que muchas personas previamente no habían considerado con respecto a la seguridad informática. Algunas organizaciones que son serias con respecto a la seguridad requieren que estas firmas sean efectuadas una vez al año. El entendimiento de las políticas puede ahora ser confirmado a través de software que examina a los trabajadores sobre las políticas que han leído.

Políticas Relacionadas: “Exámenes Sobre las Políticas” y “Clases Sobre Seguridad Informática”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

12. Clases Sobre Seguridad Informática

Política: Dentro de los tres meses siguientes a la fecha en que fue empleado en la Empresa X, cada trabajador debe asistir a una clase de toma de conciencia respecto de la seguridad informática y firmar una declaración de asistencia confirmando que ha asistido a las clases, entendido el material y que tuvo la oportunidad de hacer preguntas.

Comentario: Esta política requiere que cada nuevo trabajador asista a una clase de discusiones internas sobre seguridad informática. Para empleados regulares, una modificación de esta política puede decir que deben asistir dentro de los seis meses siguientes a la fecha de programación del curso. Para garantizar que las personas sí asisten a las clases, se les solicita que firmen una declaración reconociendo que han entendido el

material presentado. Desde un punto de vista legal, es deseable que los empleados reconozcan por escrito que entienden que la seguridad informática es parte obligatoria de su trabajo. Si son finalmente despedidos debido a una violación de la seguridad informática o problemas relacionados, no habrá duda de que el empleado entendió lo que se le requería. Por lo tanto, esta política reduce la probabilidad de una demanda de despido injustificado. Si las clases están programadas en hora de trabajo, entonces otra intención de esta política es notificar a los niveles bajos de la gerencia que deben suministrar horas de trabajo para que sus empleados asistan a los eventos de adiestramiento de seguridad informática. No hay nada de especial en la política acerca de los períodos de tiempo. Estos pueden ser cambiados para adaptarse a las necesidades y recursos de la organización. Los períodos largos de tiempo reflejan el hecho de que las clases probablemente son ofrecidas cada cierto tiempo, quizás mensualmente, pero no consecutivamente. Lo ideal sería que el material de seguridad informática fuese incluido en la orientación de los nuevos empleados, con lo cual el requerimiento de tres meses se cumpliría.

Políticas Relacionadas: “Convenio de Trabajo”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

13. Adiestramiento para Acceso al Sistema

Política: Todos los trabajadores de la Empresa X deben completar y aprobar una clase de adiestramiento en seguridad informática antes de recibir el acceso a cualquier sistema de computación de la Empresa X.

Comentario: Esta política informa a todo el personal involucrado que los nuevos trabajadores no deben recibir privilegios de acceso a ningún sistema de información de producción hasta que hayan completado una clase de adiestramiento de seguridad informática. La clase de adiestramiento no es cualquier clase de adiestramiento, sino que debe estar autorizada, cuando no redactada, por el departamento de Seguridad Informática. Esta política garantiza que cada trabajador conoce las reglas de la seguridad informática, de tal forma que pueda firmar con conciencia cualquier formulario que diga que está de acuerdo en seguir estas reglas cada vez que utilice los sistemas informáticos de la Empresa X. En algunas organizaciones, se espera que los trabajadores firmen dicha declaración sin haber asistido a la clase de adiestramiento y por lo tanto no saben con qué están de acuerdo. Esta política es fácilmente implementada a través de sistemas de

adiestramiento computarizado (SAC) disponibles en una biblioteca, salón de conferencia, centro de adiestramiento o cualquier otra área no restringida. Los nuevos empleados pueden ser enviados a esas áreas y tomar el curso a su conveniencia. Un aspecto atractivo del sistema SAC es que puede ser utilizado para medir su entendimiento del material. Una máquina de adiestramiento independiente o una red de adiestramiento es más recomendable que utilizar SAC en una intranet o red local de producción, porque las personas que reciben el adiestramiento no han obtenido para ese momento el privilegio legítimo de acceso al sistema.

Políticas Relacionadas: “Acceso para Trabajadores Temporales y Consultores” y “Adiestramiento en Seguridad Informática”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

14. Adiestramiento en Sistemas de Producción

Política: Los trabajadores de la Empresa X no deben utilizar software para los procesos de producción del negocio, a menos que hayan completado y aprobado el adiestramiento autorizado para dicho software.

Comentario: Esta política requiere que los trabajadores completen un adiestramiento autorizado previo a la utilización del software que afecta las operaciones de producción. La política está dirigida adicionalmente a asegurarse que los usuarios tienen suficiente adiestramiento antes de cambiarse a un software mejorado. Nada de lo mencionado en la política impide que los trabajadores utilicen el software en un ambiente de prueba para familiarizarse con el mismo. La política evita que los trabajadores se encuentren en una posición donde ellos pudiesen, sin querer, afectar los registros del negocio por error, omisión y fraudes, a menos que hayan completado su adiestramiento. Más allá de las interrupciones y demoras del sistema, otros riesgos que corre la empresa por usuarios adiestrados incorrectamente involucran un mal servicio al cliente y relaciones públicas adversas. Esta política evita perturbar a los usuarios que pudieran ser demasiado orgullosos como para admitir que no saben usar el software o que tienen miedo de preguntar. El adiestramiento también debe incluir la familiarización con los controles y asuntos relacionados con seguridad. La palabra "autorizado" en la política es deliberadamente vaga, permitiéndole a la gerencia suficiente flexibilidad para escoger el tipo de adiestramiento que cada sistema requiere. El hardware y la red no fueron explícitamente mencionados en esta

política porque, por implicación, redes y hardware nuevos significa software nuevo o diferente. Algunas organizaciones pudieran añadir las palabras "hardware y redes" a la política.

Políticas Relacionadas: “Tiempo de Adiestramiento”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

15. Convenio de Cumplimiento

Política: Como condición para la continuación del empleo, los empleados, consultores y contratistas deben firmar anualmente un convenio de cumplimiento de seguridad informática.

Comentario: La intención de este convenio es exigir a todos los trabajadores que firmen una declaración de cumplimiento cada año, forzándolos a reconocer sin ninguna duda que el cumplir las políticas y procedimientos de seguridad es parte de su trabajo. Estos convenios típicamente dicen que el individuo está de acuerdo en cumplir las políticas y procedimientos de seguridad de informática, que ha leído el manual de seguridad, entiende el manual y que también entiende que las infracciones son motivo para acciones disciplinarias, incluso el despido. El acto de firmar algo no sólo suministra al empleador evidencia legal admisible de que los trabajadores fueron notificados sobre la seguridad informática, sino que además cambia la percepción que los trabajadores tienen de la seguridad informática.

Políticas Relacionadas: “Acuerdos de Confidencialidad — Organización” y “Acuerdos de Confidencialidad”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

16. Adiestramiento Técnico y Educación Continua

Política: Todo el personal técnico de los sistemas informáticos debe tener suficiente adiestramiento inicial y educación continua en todos los aspectos críticos de su trabajo, incluyendo seguridad, aseguramiento de la calidad y relaciones con el cliente.

Comentario: Esta política garantiza que el personal técnico de informática obtendrá la educación y adiestramiento necesarios para efectuar un trabajo adecuado, incluyendo el hecho de hacer su trabajo con la seguridad adecuada. Una gran variedad de problemas ocurren

debido a que el personal no sabe lo que está haciendo. La solución de problemas de seguridad no debe dejarse a personal no adiestrado adecuadamente, porque sólo tratarían de adivinar qué hacer. Esta política fomenta la lealtad de los trabajadores, lo cual los animará a permanecer con su patrono. Esta política insiste en la necesidad que los empleadores paguen el adiestramiento, por lo menos para el personal de sistemas informáticos. Esta política aborda asuntos diferentes a los que normalmente se refieren otros esfuerzos de toma de conciencia relativos a seguridad informática.

Políticas Relacionadas: “Alertas Sobre Vulnerabilidades” y “Adiestramiento en Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

17. Responsabilidad en la Seguridad Informática

Política: La responsabilidad de la seguridad informática del día a día debe ser tarea de cada trabajador y no sólo del departamento de Seguridad de Informática.

Comentario: El propósito de esta política es aclarar el hecho de que la seguridad informática es multidisciplinaria, multidepartamental y multiorganizacional por naturaleza. Esto quiere decir que un solo departamento dentro de la Empresa X no puede abordar adecuadamente la seguridad informática. Cada trabajador debe

hacer su parte con el propósito de alcanzar los niveles apropiados de seguridad informática. Después de todo, la información se encuentra en todas partes de la organización y casi todos los trabajadores utilizan la información para efectuar su trabajo. Es pues natural que todo trabajador asuma su cuota de responsabilidad por la seguridad informática. Algunas organizaciones dan un paso más allá de esta política, e incorporan en los formularios de evaluación del desempeño la pregunta respecto a si el empleado cumple la política de seguridad informática en el transcurso de su trabajo. Para ser verdaderamente efectiva, esta política se debe complementar con instrucciones adicionales, diciendo a los trabajadores lo que de ellos se espera. Esto normalmente aparecería en material de toma de conciencia, aunque se recomienda que también aparezca en las descripciones de cargos. Esta política es normalmente seguida por instrucciones orientadas a los usuarios en materia de escogencia de contraseñas fuertes o en el sentido de no divulgar la contraseña a otras personas. La importancia de esta política crece a medida que se utilizan sistemas distribuidos para actividades de procesamiento informático porque aumenta la dependencia que se tiene en los usuarios.

Políticas Relacionadas: “Evaluaciones de Desempeño” y “Tareas del Departamento de Seguridad Informática”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6.03 Respuesta a Incidentes y Anomalías de Seguridad

6.03.01 Reporte de Incidentes de Seguridad

1. Pérdida o Divulgación de Información Sensible

Política: Si la información sensible se pierde o se divulga a personas no autorizadas, o existe una sospecha de haberse perdido o divulgado a terceros no autorizados, tanto su Propietario como el personal apropiado de Seguridad Informática deben ser notificados inmediatamente.

Comentario: Es necesaria la pronta notificación de la pérdida o divulgación de la información confidencial. Por ejemplo, si la información sobre un producto nuevo, pero que no se ha publicado, se ha divulgado a un reportero por error, entonces la fecha para el anuncio oficial del producto debe cambiarse. La intención de la

política es por lo tanto requerir que todos los trabajadores reporten la pérdida o divulgación de información sensible. Esta política funciona mejor cuando la palabra “sensible” ha sido explícitamente definida dentro de la organización a través del sistema de clasificación de datos. Asimismo, la terminología “Propietario de la Información” debe ser definida en otra parte.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Propiedad de la Información,” y “Notificación de Falla en los Controles de la Integridad”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Divulgación de las Vulnerabilidades del Sistema Informático

Política: La información específica sobre las vulnerabilidades del sistema informático, tales como los detalles de una reciente intromisión en el sistema, no deben ser distribuidas a personas que no tienen una necesidad demostrada de conocerla.

Comentario: Esta política permite saber a las pocas personas que tienen acceso a la información sobre vulnerabilidades del sistema informático, que la divulgación de esta información debe estar estrictamente controlada. Si la vulnerabilidad informática cae en manos de personas no autorizadas, estas personas podrían utilizarla para comprometer los sistemas de la organización. Estas personas no autorizadas también pueden utilizarla para extorsionar o públicamente poner en aprietos a la organización. Dicha información también puede ser de interés y utilidad para batallas políticas internas. La vulnerabilidad de la información también puede erosionar la confianza que los usuarios y la gerencia tienen en el Departamento de Sistemas Informáticos y por esta razón también debe ser restringida. Algunas organizaciones van más lejos que esta política. Por ejemplo, pueden requerir que la vulnerabilidad de los sistemas informáticos sea etiquetada con palabras especiales para restringir el acceso. Similar a las etiquetas de clasificación de datos tales como "secreto", estas etiquetas de advertencia pueden ser muy específicas, prohibiendo la distribución en boletines electrónicos y sistemas públicos. Otras organizaciones pueden tener un registro de las personas que recibieron esta información y cuándo fue devuelta.

Políticas Relacionadas: "[Código Fuente del Software de Penetración de Sistemas](#)" y "[Presentación de la Imagen Pública](#)"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Notas de Prensa Sobre Información de Vulnerabilidad

Política: Las notas de prensa u otras declaraciones públicas dadas por la Empresa X que contengan información sobre la vulnerabilidad informática, no deben contener detalles específicos.

Comentario: Esta política evita que los representantes de la Empresa X causen problemas por haber publicado detalles específicos sobre la vulnerabilidad informática. Si se dan detalles específicos, se permitiría que los

hackers y otros lancen ataques en contra de otros sitios y la Empresa X puede ser señalada como la responsable por los daños ocasionados. Abstenerse de divulgar estos detalles puede ser frustrante para los medios de comunicación, pero ayudará a que el método de ataque no sea utilizado nuevamente en contra de los sistemas de la Empresa X. La divulgación pública de estos detalles puede adicionalmente informar a los delincuentes que se conoce cierta información sobre ellos e inducirlos a destruir ciertas pruebas que pudieran utilizar los investigadores en un juicio. La divulgación de los detalles de los delitos de computación también anima a los delincuentes a escapar para evitar el arresto. Esta política adicionalmente ayuda a los representantes de la Empresa X a no especular acerca de la forma cómo se hizo el ataque, lo cual puede evitar demandas por difamación y calumnia. La divulgación a proveedores importantes y a agencias gubernamentales que persiguen a los hackers de computadores no está cubierta por esta política y por ende es permitida.

Políticas Relacionadas: "[Presentación de la Imagen Pública](#)" y "[Código Fuente del Software de Penetración de Sistemas](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Explotación de la Vulnerabilidad del Sistema y Datos de la Víctima

Política: El personal de la Empresa X no debe divulgar información acerca de individuos, organizaciones, métodos específicos utilizados para sacar provecho, o sistemas específicos que han sido dañados por delitos y abusos en computación.

Comentario: Esta política es apropiada para proveedores de productos y servicios para sistemas informáticos. Por ejemplo, un proveedor de estaciones de trabajo puede publicar información sobre la existencia de un problema de seguridad y cómo instalar un parche para solventar el problema, pero los clientes que fueron víctima y la forma en que fueron cometidos los ataques deben mantenerse confidenciales. Esta política garantiza que terceros no autorizados no utilizarán la información para montar ataques adicionales en contra de las víctimas porque no sabrán quiénes son, ni qué sistemas están involucrados ni los detalles de los ataques. Esto también dificulta aún más a las personas no autorizadas el aprovechamiento de la vulnerabilidad porque deben descubrir el método específico de ataque.

Políticas Relacionadas: “Solicitudes Externas de Información” y “Divulgación de las Vulnerabilidades del Sistema Informático”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

5. Problemas en el Sistema de Producción

Política: Todos los errores importantes, los procesamientos incompletos y los procesamientos impropios de las aplicaciones de producción, deben ser inmediatamente reportados al Centro de Atención al Usuario.

Comentario: Esta política alerta al personal técnico en el sentido de que algo anda mal en las aplicaciones de producción. Estos problemas pueden ser más serios que un simple error de programación. Pueden ser, por ejemplo, una indicación del ataque actual de un hacker, o de datos viciados o de sistemas no confiables. El requerimiento del reporte de todos los problemas significativos también evita que los usuarios racionalicen que el problema ya es conocido por el personal técnico, o que otros ya lo han reportado. Esta política también suministra un criterio nuevo y diferente para determinar si las aplicaciones se ejecutaron exitosamente hasta completarse. Esto es deseable porque el usuario tiene una perspectiva de negocios que la mayoría de las personas del departamento de tecnología de información no posee.

Políticas Relacionadas: “Condiciones de Interrupción” y “Daño y Pérdida de Sistemas Fuera de Sede”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Bromas en Seguridad Informática

Política: Los trabajadores no deben jugar o hacer travesuras, o de alguna otra manera humorística hacer ver que está ocurriendo un incidente de seguridad, o va a ocurrir, u ocurrió, cuando tal cosa no es cierta.

Comentario: Esta política es similar a la adoptada por aeropuertos en todo el mundo, mediante la cual es un delito serio bromear diciendo que se tiene un cuchillo, o pistola o cualquier otro tipo de arma. Lo que sucede cuando hacen esto es causar una falsa alarma que no sólo desperdicia recursos y ocasiona malestar innecesario a las personas, sino que posiblemente sirve como distracción para ataques reales. Esta política evita las comunicaciones y las interpretaciones erróneas.

Políticas Relacionadas: “Páginas Web No Oficiales” y “Recopilación de Datos Personales Bajo Pretextos”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

7. Mensajes Ofensivos de Correo Electrónico

Política: Todos los trabajadores deben responder directamente a la fuente de mensajes electrónicos, llamadas telefónicas y otras comunicaciones ofensivas y, de no cesar los mensajes ofensivos, los trabajadores deben reportar las comunicaciones a su gerente y al departamento de Recursos Humanos.

Comentario: Esta política está dirigida a estimular a los trabajadores a tratar directamente con la fuente del material que consideran ofensivo. Sólo cuando la fuente falla en tomar medidas por la reacción, entonces deberán los trabajadores pasar la información a su gerente o al departamento de Recursos Humanos. En muchas ocasiones, la fuente no considera que cierto material es ofensivo y una simple queja es suficiente para acabar con las comunicaciones no deseadas. Una fuente puede ser un individuo que simplemente reenvía material obtenido de otra fuente. La existencia de esta política es un indicador que una organización toma en serio los asuntos legales, como el acoso sexual o un ambiente hostil de trabajo. Esta política demuestra que la gerencia es tan seria en este asunto, que ha establecido un proceso para su resolución.

Políticas Relacionadas: “Remoción de Material Ofensivo” y “Acoso Sexual, Etnico y Racial”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

8. Daño y Pérdida de Sistemas Fuera de Sede

Política: Los trabajadores deben reportar prontamente a sus gerentes en la Empresa X cualquier daño o pérdida de hardware, software o información confiada a ellos.

Comentario: Esta política garantiza que los teletrabajadores y los trabajadores con computadores portátiles reportarán cualquier daño o pérdida con prontitud. Esto permitirá tomar las medidas necesarias, tal como remplazar un computador portátil inmediatamente, para así minimizar el impacto en la actividad de negocio. Esto también permitirá la pronta notificación al Propietario de la información, en caso de que se haya perdido información sensible. La política puede ser aumentada con otra oración que diga que se exige a los

gerentes departamentales reportar estos daños o pérdidas al departamento de Seguridad Física, el cual generalmente guarda un registro de pérdidas. Alternativamente, se puede pedir a los usuarios que reporten todos los daños o pérdidas al Centro de Atención al Usuario, la cual a su vez reportará a los grupos internos correspondientes, incluyendo el departamento de seguros, que luego cobrará el seguro por los computadores portátiles robados. En muchos casos, el usuario que reporta la pérdida tendrá que llenar un reporte de pérdida, pero debido a que es un procedimiento, no está detallado en la política. Esta política requiere que se reporten las pérdidas y daños a la información. Esto es un asunto particularmente importante para organizaciones involucradas en espionaje y robos de computadores portátiles. Esta política está deliberadamente redactada de tal manera que se pueda aplicar a todas las instalaciones, no sólo a los sistemas fuera de sede.

Políticas Relacionadas: “[Informes de Incidentes](#)” e “[Informes de Violaciones y Problemas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Informes de Incidentes

Política: Todas las sospechas de incidentes de seguridad informática deben ser reportadas tan pronto sea posible, a través de los canales internos autorizados de la Empresa X.

Comentario: Con esta política se intenta que todos los problemas e infracciones sean prontamente informados a quienes realmente puedan hacer algo al respecto. Si las infracciones y los problemas no son reportados, pueden acarrear pérdidas mayores para la organización que si se hubiesen reportado a tiempo. Un buen ejemplo de esto son los virus de computadores que, si no son reportados a tiempo, continuarán propagándose. Algunas organizaciones van más allá, exigiendo que el reporte se haga dentro de un límite de tiempo, por ejemplo 24 horas. Otras organizaciones añaden multas específicas por no reportar los problemas. La ejecución de esta política puede involucrar un número de teléfono público gratuito para evitar pagar la llamada. Para estimular los reportes, el anonimato se puede lograr parcialmente apagando el identificador de llamadas del teléfono receptor. Igualmente, el departamento de Seguridad Informática puede publicar el hecho de que los reportes pueden ser efectuados de manera anónima. También puede animar a la gente saber que siempre contestará una contestadota automática, nunca una persona. Se hace referencia a

“canales autorizados” para estimular a las personas a ir a Seguridad Informática u otras personas reconocidas como responsables de las investigaciones. Las palabras “canales autorizados” también estimulan el establecimiento de tales canales para el flujo de información si no han sido definidos todavía.

Políticas Relacionadas: “[Daño y Pérdida de Sistemas Fuera de Sede](#),” “[Informes de Violaciones y Problemas](#),” “[Sistema de Alerta de Seguridad Informática](#),” “[Investigaciones Prolongadas](#),” e “[Infracción de la Ley](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Severidad de los Incidentes Reportados

Política: A menos que razonablemente se suponga que la pérdida puede continuar, un incidente de seguridad informática con daños inferiores a \$100 y que haya sido resuelto por las personas involucradas, no tiene que ser reportado al departamento de Seguridad Informática.

Comentario: Esta política establece el umbral financiero para el reporte de incidentes de seguridad informática. El uso de ese umbral permite al departamento de Seguridad Informática enfocarse en aquellos asuntos que son más importantes para la organización. Una gran deficiencia de esta política es que la decisión de si se reporta o no, queda en manos de personas que generalmente tiene muy poca experiencia en el área de seguridad. Esto nos lleva a una situación en la que la persona que debe reportar el incidente, no lo reporta porque no entiende la seriedad del problema o el alcance de los daños. Por esta razón, la política no se recomienda. Es generalmente preferible que sea el personal de Seguridad Informática el que determine cuáles incidentes requieren atención adicional. Esta política la utiliza de mejor manera la gerencia de Seguridad de Informática que busca continuamente ampliar su personal. El gerente en tal situación podría declarar que la política es necesaria porque el personal actual es sobrepasado por los incidentes que se reportan, y que es necesaria alguna forma de priorización. Cuando la gerencia se involucra en una discusión de esta propuesta, pueden enfatizarse los efectos secundarios indeseables que acompañan esta política. Por tal motivo, la alta gerencia debe optar por incrementar el personal para investigar adecuadamente todos los incidentes que se reportan. Es importante en otra política o en cualquier otra documentación definir qué constituye un incidente. No hay nada especial acerca del umbral de \$100; pudo haber sido de \$1.000.

Políticas Relacionadas: "Informes de Incidentes" e "Informes de Violaciones y Problemas"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

11. Informes de Violaciones y Problemas

Política: Los trabajadores de la Empresa X tienen la obligación de reportar todas las infracciones y problemas de seguridad informática al departamento de Seguridad de Informática oportunamente, para que se tomen las acciones correctivas correspondientes.

Comentario: Esta política requiere que los trabajadores reporten prontamente las infracciones y problemas de seguridad informática. Por ejemplo, reportar de inmediato es absolutamente esencial para evitar las pérdidas ocasionadas por penetraciones no autorizadas al sistema y otros problemas de seguridad potencialmente serios. La demora en reportarlas puede significar pérdidas masivas adicionales para la organización. Esta política reconoce que las personas que usan los sistemas son normalmente los que detectan los problemas. Esta política requiere que los problemas sean reportados a alguien que pueda hacer algo al respecto. Aquí el proceso de reportar se hace a un grupo central en vez de a la gerencia de línea o un proveedor de servicio. El proceso de reportar también podría ir a través de la gerencia de línea, pero esto toma más tiempo y es probable que las acciones correctivas sufran demoras. La política puede ser ampliada para decir que los trabajadores no deben, bajo ninguna circunstancia, intentar demostrar la existencia de estas debilidades, a menos que sean específicamente asignados a este tipo de trabajo por la alta gerencia. Esta advertencia pudiera ser agregada para disuadir las intromisiones al sistema que pudiesen ser interpretadas como mal uso del sistema. Esta política puede ser ampliada para requerir un reporte escrito después del reporte oral inicial. El alcance de esta política puede ser ampliado para incluir "sospecha de problemas", no sólo "infracciones y problemas". La palabra "debilidades" también podría ser usada en vez de "problemas". Así como el reportar internamente se estimula y se requiere, el reportar externamente está repleto de peligros importantes.

Políticas Relacionadas: "Reportes Externos de Violaciones," "Equipo de Respuesta Ante Emergencias Computacionales," e "Informe de Sospecha de Virus"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Alternativas para el Reporte de Violaciones y Problemas

Política: Los trabajadores de la Empresa X deben reportar inmediatamente todas las sospechas de problemas, vulnerabilidades e incidentes de seguridad informática a su gerente inmediato o a la gerencia de Seguridad Informática.

Comentario: Esta política brinda al trabajador múltiples vías para reportar problemas, vulnerabilidades e incidentes de seguridad informática. Si, por ejemplo, el problema involucra al departamento de Seguridad Informática, reportarse a sí mismos sería problemático. Igualmente, si el asunto involucra al gerente del trabajador, el reportarlo al mismo gerente sería inconveniente. Este enfoque de dos vías garantiza que toda la información importante se comunica y no se retiene porque la persona que lo reporta teme posibles repercusiones políticas u otros problemas potenciales. El uso de esta política requiere que se establezcan vías adicionales de comunicación para permitir a los gerentes pasar la información de forma expedita al departamento de Seguridad Informática, al Centro de Atención al Usuario, al Equipo de Respuesta ante Emergencias Computacionales o a cualquier otro grupo que esté en capacidad de tomar acción inmediata. Esta política funciona mejor si una de esas vías para reportar es anónima.

Políticas Relacionadas: "Informes de Incidentes" y "Cambios en Situación de Usuarios"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

13. Interferencia con Reportes de Violaciones y Problemas

Política: Los trabajadores nunca deben intentar interferir, impedir, obstruir o disuadir a un integrante del personal en su esfuerzo por reportar la sospecha de algún problema o infracción en la seguridad informática, o tomar represalias en contra de un individuo que reporte o investigue infracciones o problemas en seguridad informática.

Comentario: Esta política estimula a los trabajadores que desean reportar una violación o problema de Seguridad Informática, pero les preocupa que pueda ser difícil de realizar. Aquellos que avisan de asuntos sospechosos frecuentemente se muestran preocupados de que su gerencia inmediata los penalice por reportar problemas o infracciones. Esta política trata de fomentar

una perspectiva que está dirigida al mejor interés de la organización, en vez del interés político interno de algún gerente.

Políticas Relacionadas: “[Informes de Problemas](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

14. Protección para Reportes de Violaciones y Problemas

Política: La Empresa X debe proteger los trabajadores que en buena fe reporten lo que consideren una violación de las leyes o reglamentos o condiciones que puedan poner en peligro la salud o seguridad de otros trabajadores.

Comentario: Esta política garantiza protección para los trabajadores que están considerando reportar problemas. Esto debe animar a los trabajadores a hacer el reporte cuando han estado inclinados a no hacerlo a causa de las potenciales consecuencias adversas. Más allá de eso, la política también instruye a los trabajadores para reportar los problemas internamente en vez de externamente, reduciendo así la publicidad adversa y pérdida de confianza del cliente. Esta política no prohíbe los reportes externos. Sólo indica que el problema debe ser reportado internamente y el trabajador debe dar algún tiempo a la Empresa X para solucionar la situación. Nada de lo mencionado en esta política impide que la Empresa X despida al trabajador por otras razones, tales como un mal desempeño en otras áreas. La política está deliberadamente definida de manera amplia, con el fin de incluir los problemas de Seguridad Informática. También incluye problemas de seguridad física y problemas de seguridad del trabajador.

Políticas Relacionadas: “[Reportes Externos de Violaciones](#)”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

15. Identidad del Informante de Violaciones y Problemas

Política: Los trabajadores que reporten al departamento de Seguridad un problema de seguridad, vulnerabilidad, o una condición no ética dentro de la Empresa X pueden, a su discreción, mantener su identidad en estricta reserva.

Comentario: Esta política estimula a los denunciantes a revelar irregularidades, problemas de control y otros asuntos de seguridad. En muchos casos los denunciantes no dicen nada porque tienen miedo de que, como consecuencia del reporte, puedan perder su trabajo o sufrir un revés en su carrera. Esta política limita pero no elimina la posibilidad de que el denunciante sufra ese destino. Si bien los buzones de sugerencias, las llamadas telefónicas anónimas y otros mecanismos de reportes anónimos pueden estar disponibles sin una política como ésta, los denunciantes potenciales pueden inhibirse porque temen que se conozca su identidad durante el transcurso de una investigación. Al dar a conocer su identidad a Seguridad Informática, los denunciantes pueden recibir trato especial al conocerse que ellos han tomado parte en la solución del problema. La política podría ser ampliada para incluir palabras que digan que se mantendrá informado al denunciante durante el proceso de investigación y su avance. Esto adicionalmente estimula a las personas a hacer las denuncias, porque si piensan que no se va a hacer nada no se animarán a realizar las denuncias.

Políticas Relacionadas: “[Protección para Reportes de Violaciones y Problemas](#)” y “[Reportes Centralizados de Problemas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

16. Reportes Externos de Violaciones

Política: A menos que la ley o los reglamentos exijan reportar las infracciones de seguridad informática a las autoridades externas, la gerencia, conjuntamente con representantes del departamento Legal, del departamento de Seguridad Informática, del departamento de Seguridad Física y del departamento de Auditoría Interna, deben sopesar las ventajas y desventajas de una divulgación externa antes de reportar las infracciones.

Comentario: Muchas organizaciones se abstienen de reportar delitos de computación porque la vergüenza pública, el costo y la desviación de recursos de personal sobrepassan los beneficios. Los beneficios incluyen establecer un ejemplo para desanimar otras infracciones,

lo cual da a los empleados la impresión de que la gerencia cree en el sistema de justicia criminal y en obtener restituciones. Con frecuencia es deseable que la gerencia reciba la oportunidad de escoger reportar las infracciones caso por caso. Esta política requiere que la gerencia estudie las ventajas y desventajas de cada caso antes de hacer un reporte externo, siempre y cuando las leyes locales brinden a la gerencia esa flexibilidad. Aunque es poco frecuente, algunas organizaciones podrían establecer un comité que evalúe los méritos de un reporte externo tomando caso por caso. Las policías y los investigadores apoyan los reportes públicos porque necesitan estadísticas para lograr un mejor entendimiento de la naturaleza del delito. Por el momento, un gran número de delitos de computación no son reportados y otro número importante de ellos pasan desapercibidos. El requerimiento de reportes externos está restringido a las infracciones de las leyes y reglamentos, mientras que los reportes internos pueden incluir infracciones a las políticas y otros abusos que no son necesariamente ilegales. La política aquí prevista tiene un alcance reducido porque se refiere a infracciones a la seguridad informática. La política puede ser ampliada para enfocar todas las infracciones relacionadas con la seguridad.

Políticas Relacionadas: “Retención de la Información Sobre Violaciones y Problemas de Seguridad,” “Informes de Violaciones y Problemas,” e “Informes de Problemas”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

17. Reporte de Violaciones y Problemas a las Autoridades

Política: Cualquier evento potencialmente material debe ser reportado por la gerencia de Seguridad Informática al vicepresidente del departamento Legal y al vicepresidente del departamento de Finanzas, quienes deben decidir si la divulgación pública es necesaria y apropiada.

Comentario: De acuerdo con las leyes de seguridad de un país, eventos negativos importantes deben ser dados a conocer al público con prontitud. Estos eventos típicamente se caracterizan por ser cualquier información importante que pudiera afectar el proceso de decisión del inversionista. El asunto aquí es si el inversor considera que la información afecta su toma de decisión. Si la toma de decisión se ve afectada, entonces el evento debe ser publicado. De no ser así, los detalles del evento son retenidos internamente. La mayoría de las organiza-

ciones callan las malas noticias por temor que ello puede impactar su imagen, la confianza del cliente, la confianza del proveedor, la moral del empleado y otros factores. Pero ciertas compañías han sido afectadas por demandas de los accionistas que alegan demoras o reportes insuficientes de eventos adversos. Esta política requiere que la gerencia considere las divulgaciones, ponga atención a las leyes importantes sobre divulgación y establezca un proceso formal para manejar estas divulgaciones. Mediante la acción rápida y correcta, la gerencia puede evitar o desviar demandas judiciales por parte de los accionistas. Mediante el uso de esta política, la gerencia puede también evitar una caída severa en el precio de las acciones, causada por la pérdida de la confianza del accionista, debido a las revelaciones en detalle sobre el problema originado, porque inicialmente se suprimió la información. Se requieren otras estructuras organizacionales para reportar otros tipos de eventos materiales, como la reducción de personal. Esta política se aplica primordialmente a compañías que se cotizan en el mercado de valores, pero también puede ser reformulada para otras organizaciones para que tomen en consideración cosas que la comunidad local debe saber.

Políticas Relacionadas: “Reportes Externos de Violaciones”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

18. Divulgación de Ataques a Sistemas de Computación

Política: A menos que esté obligada por ley a publicar ataques contra sus sistemas o redes de computación, la Empresa X no debe reportar estos incidentes al público o a agencias gubernamentales.

Comentario: Esta política mantiene a las organizaciones fuera de los periódicos si las van a mencionar desfavorablemente. Esto mantiene alta la confianza del cliente y evita que se afecten los precios de las acciones. Para organizaciones en industrias reguladas, tales como agua, electricidad y transporte, esta política intenta mantenerlas fuera de problemas con respecto a los reglamentos. Además, la política reconoce que la mayoría de los gobiernos no tienen un mecanismo seguro y confiable para proteger la información sobre ataques. Compartir información sobre ataques con una agencia del gobierno puede ser irresponsable porque puede llevar al aprovechamiento no autorizado de esta información. Muchas organizaciones mantienen un bajo perfil y no publican información sobre ataques. Esta

política frecuentemente no está escrita, pero en muchas situaciones puede ser recomendable ponerla por escrito para evitar que trabajadores la publiquen. Otra buena razón para poner esta política por escrito es demostrar que es un enfoque legítimo y justo, no una regla decisiva que debe ser escondida. La política deliberadamente no hace distinciones entre un ataque exitoso y uno fallido, donde ambos pueden incluir información sensible.

Políticas Relacionadas:“[Reportes Externos de Violaciones](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Reportes de Brechas de Seguridad a Terceros

Política: Cualquier brecha en la seguridad de un computador de la Empresa X que exponga información privada o propiedad de terceros, debe ser comunicada inmediatamente a la parte afectada.

Comentario: Esta política proporciona a la gerencia interna de la Empresa X, instrucciones sobre cuándo debe reportar a terceros las intrusiones en la seguridad del computador. Por ejemplo, si la base de datos de tarjetas de crédito de un comerciante de la web ha sido expuesta porque los hackers entraron a su página comercial en Internet, entonces el comerciante tiene el deber de informar no solamente a los clientes involucrados, sino también a los emisores de las tarjetas de crédito. Las organizaciones deben planificar por anticipado cómo manejar una brecha de seguridad, y esta política es una consideración en dicho proceso de planificación. La política se aplica a una amplia variedad de amenazas, incluyendo el robo de identidad y la expropiación de información patentada.

Políticas Relacionadas:“[Reporte de Violaciones y Problemas a las Autoridades](#)” y “[Reportes Externos de Violaciones](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

20. Informes de Actividad No Autorizada

Política: Los usuarios de los sistemas informáticos de la Empresa X deben inmediatamente reportar a la gerencia de Seguridad Informática cualquier actividad no autorizada incluyendo, sin limitantes, la pérdida o

cambios en los datos computarizados de producción y el uso cuestionable de archivos, bases de datos, o redes de comunicación.

Comentario: Esta política brinda a los usuarios ejemplos específicos de los tipos de eventos que deben ser reportados a la gerencia de Seguridad Informática. La política logra la participación de usuarios en un equipo de seguridad informática y la utiliza para detectar eventos inusuales que pueden ser indicativos de sabotaje, fraude, mal funcionamiento del sistema y otros eventos relevantes de seguridad informática. La política puede necesitar explicaciones adicionales cuando sea entregada a la comunidad de usuarios finales.

Políticas Relacionadas:“[Informe de Funcionamiento Incorrecto de Software](#),” “[Informes de Violaciones y Problemas](#),” y “[Reportes Centralizados de Problemas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

21. Reporte de Eventos Cuestionables

Política: Los usuarios de los sistemas informáticos de la Empresa X deben reportar inmediatamente al departamento de Seguridad Informática cualquier evento inusual o información sospechosa relativa a la seguridad informática incluyendo, sin limitantes, solicitudes inusuales de información de la Empresa X efectuadas por personas externas y la conducta atípica del sistema.

Comentario: Esta política informa a los usuarios y personal técnico, que deben reportar eventos inusuales. Un ejemplo sería un mensaje de bienvenida indicando el último identificador de usuario que fue utilizado en fechas y horas específicas, cuando el usuario sabe que no utilizó el sistema en la fecha y hora mencionadas. Tal discrepancia puede indicar que la hora del reloj interno del computador se debe revisar, o que alguna persona no autorizada está utilizando el identificador de usuario. Esta política es particularmente importante cuando se trate de solicitudes de información interna, sea por correo electrónico, por teléfono, casualmente en una reunión de una sociedad profesional, o por otra parte porque estas mismas solicitudes pueden ser indicativas de intentos de ingeniería social. Cuando el departamento de Seguridad Informática tiene este tipo de información a su disposición, podrá determinar si está presente una amenaza genuina, y si se requiere tomar correctivos adicionales. Esta acción correctiva puede incluir un memo dirigido a todo el personal, informándoles de los ataques de ingeniería social que se han descubierto.

Políticas Relacionadas: “Investigaciones Policiacas o Legales” y “Solicitudes de Información Organizacional”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

22. Reporte de Problemas en Diseño

Política: Todos los problemas potencialmente serios asociados con sistemas informáticos en diseño o desarrollo, que no se han abordado adecuadamente por los proyectos existentes o planificados, deben ser reportados inmediatamente a la gerencia de Seguridad Informática.

Comentario: Esta política otorga a los trabajadores un canal de reporte aparte del existente en la jerarquía normal con el cual normalmente operan. Los canales normales de reporte frecuentemente no son suficientes para reportar problemas mayores porque a la gerencia no le gustan las malas noticias, no quiere verse mal, no quiere gastar dinero ahora cuando pueden gastarlo posteriormente, o no tienen la pericia técnica para entender el problema. Esta política requiere oficialmente que los integrantes del personal técnico lleven los problemas a la atención de la gerencia de Seguridad Informática. Como alternativa puede utilizarse al gerente de Auditoría Interna. La naturaleza de los problemas no ha sido definida. Dejando esta palabra ambigua, la política cubre un rango muy amplio de posibles problemas. Esta política establece que todas las personas a lo largo de la organización son responsables por la seguridad informática, no sólo los integrantes de departamento de Seguridad Informática. Este proceso de reporte puede proceder anónimamente, por ejemplo a través de una línea dedicada, que se conecta a una máquina contestadora sin identificador de llamadas.

Políticas Relacionadas: “Diseño de Controles de Seguridad Informática” y “Excepciones a las Políticas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

23. Contacto con las Autoridades Policiales

Política: Toda decisión sobre incidentes o problemas de seguridad informática que involucre o amerite contacto con las autoridades policíacas, debe ser tomada por un representante corporativo de la Empresa X.

Comentario: Esta política evita serias interrupciones a los negocios que adopten esta política por parte del personal técnico y usuarios bien intencionados. Cuando

los organismos policiales son involucrados en una investigación, pueden hacer una cantidad de cosas que ocasiona que el negocio se detenga, o al menos hacer que se incurra en costos adicionales significativos. Por ejemplo, estos organismos pueden incautar los computadores involucrados como evidencia y esto significa que las máquinas no estarán disponibles para efectuar sus actividades regulares. Cuando estos organismos se involucran, la organización víctima pierde el control del caso. Por ejemplo, no podrá decidir si el caso será llevado a la corte. Igualmente, el proceso legal de ayudar a estos organismos en las investigaciones y en el proceso consume más tiempo y gastos que lo que la gerencia interna desea. Otra razón para ser cauteloso en la decisión de involucrar a estos organismos es que ellos pueden estar sujetos a ciertas leyes de privacidad, pero no los investigadores internos.

Políticas Relacionadas: “Informes de Problemas” y “Responsabilidad en la Seguridad Informática”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

24. Investigación de Delito Computarizado

Política: Cada vez que se evidencie claramente que la Empresa X ha sido víctima de un delito de computación o de comunicación, se debe efectuar una investigación profunda que contenga suficiente información, de manera que la gerencia pueda tomar acciones para asegurarse que tales incidentes no vuelvan a ocurrir, y que se han restablecido medidas efectivas de seguridad.

Comentario: Esta política esta orientada a garantizar que la gerencia tomará la acción apropiada como respuesta a delitos de computación o de comunicación. Con mucha frecuencia la gerencia se inclina a no hacer nada porque no sabe qué hacer. Para evitar que la gerencia trate de contener información sobre vulnerabilidades, frecuentemente por supuestas ramificaciones negativas, esta política requiere que la gerencia misma inicie una investigación. En la mayoría de los casos, las gerencias de departamentos y locales no tienen la pericia para llevar a cabo la investigación. La política indirectamente requiere que estos gerentes contacten al departamento de Seguridad Informática, Auditoría Interna u otro grupo con la experiencia necesaria. La política también protege contra demandas que aleguen que la gerencia no se ocupó del problema, a pesar de haber sido notificados de la existencia de un problema de seguridad. Ejemplos de delitos de computación y de comunicación que podrían ser aptos para ser incluidos en una explicación adjunta incluyen el robo de secretos

industriales residentes en el computador y fraudes en sucursales telefónicas. Algunas organizaciones pueden desear llevar esta política un paso más adelante requiriendo investigaciones con la sola sospecha. Otra variación en la política es el requerir que una investigación se abra después de observado un abuso, aun cuando dicho abuso no sea legalmente un delito. Este procedimiento requiere la definición del término "abuso". Un ejemplo de un abuso en computador que no es un delito en muchas jurisdicciones es la violación de la privacidad. Reportar tales incidentes al comité de auditoría en la junta directiva puede ser obligatorio por efecto de la política.

Políticas Relacionadas:“Confidencialidad de la Información de las Investigaciones Internas”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

25. Investigaciones Prolongadas

Política: Las investigaciones prolongadas de brechas de seguridad se deben efectuar mientras el trabajador sospechoso esté suspendido sin paga, y la razón de la suspensión sin paga no debe ser divulgada a los compañeros de trabajo sin el expreso permiso del director de Seguridad.

Comentario:Esta política suministra a la gerencia tiempo para recopilar la información necesaria para determinar si el empleado en cuestión perpetró el supuesto delito o abuso. Debido a que las investigaciones cortas no necesitan suspensiones sin paga, se utiliza en la política la palabra "prolongada". Por cuanto la política es deliberadamente vaga, la gerencia puede decidir prolongar las investigaciones caso por caso. Teniendo al empleado sospechoso fuera del sitio de trabajo se evita que evidencia importante sea escondida, modificada o destruida. La política también previene

juicios anticipados sobre la culpabilidad o inocencia del empleado involucrado, y esto es deseable porque impide demandas por difamación y el requerimiento de confidencialidad impide aún más este tipo de demanda. Una alternativa recomendada es la suspensión con paga en lugar de suspensión sin paga, ya que si el empleado resulta ser inocente, habrá poco o ningún resentimiento.

Políticas Relacionadas:“Responsabilidades en el Manejo de Incidentes” e “Informes de Incidentes”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

26. Distintivos de Acceso Extraviados

Política: Todo dispositivo de acceso faltante incluyendo, sin limitantes, distintivos de identificación, tarjetas de acceso físico, tarjetas inteligentes con contraseñas dinámicas y tarjetas telefónicas, que esté extraviado o no sea localizable, se debe reportar inmediatamente al departamento de Seguridad Física.

Comentario:Esta política requiere que los trabajadores notifiquen al departamento de Seguridad Física, sobre cualquier pérdida o robo de distintivos o tarjetas portátiles. Seguridad Física podrá entonces tomar medidas para obstaculizar los privilegios asociados con estos distintivos o tarjetas portátiles. De esta manera pueden minimizarse las pérdidas ocasionadas por distintivos o tarjetas portátiles robadas o perdidas. Las palabras "departamento de Seguridad Física" pudieran ser "departamento de Seguridad Informática" u otras palabras que reflejen otra unidad organizacional.

Políticas Relacionadas:“Uso de Tarjetas de Crédito” y “Credenciales Portátiles de Identificación”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

6.03.02 Reporte de Debilidades en la Seguridad

1. Informe de Vulnerabilidades del Sistema

Política: Los usuarios deben reportar con prontitud todos los alertas de seguridad informática, las advertencias y sospechas de vulnerabilidades al Centro de Atención al Usuario de Sistemas Informáticos, y no deben compartir dicha información con personas internas o externas.

Comentario:Esta política evita que los usuarios bien intencionados ocasionen preocupación y trastorno innecesarios en la comunidad usuaria. Esta política se ha convertido recientemente en una necesidad para muchas organizaciones porque se han reportado muchos engaños. La política indica que el Centro de Atención al Usuario servirá de filtro para tales informaciones, desechariendo engaños, reportes inexactos de problemas y problemas viejos que ya han sido resueltos. El Centro de

Atención al Usuario está también en una mejor posición que un usuario final para contactar a las personas que necesitan saber al respecto. Para hacer que esta política funcione mejor, el Centro de Atención al Usuario, que a menudo está de guardia 24 horas al día, 7 días a la semana, debe ser capaz de movilizar instantáneamente un equipo de respuesta ante emergencias computacionales. El Centro de Atención al Usuario adicionalmente verifica firmas digitales y direcciones remitentes válidas de correo electrónico de los grupos oficiales de respuesta ante incidentes, para certificar la validez de los problemas reportados. Esta política evita que los usuarios bien intencionados hagan representaciones falsas de la seguridad de los sistemas a grupos externos.

Políticas Relacionadas: “Equipo de Respuesta Ante Emergencias Computacionales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Condiciones de Interrupción

Política: Los trabajadores deben notificar a la gerencia con prontitud de todas las condiciones que pudieran llevar a una interrupción de las actividades del negocio.

Comentario: Esta política requiere que los trabajadores se mantengan atentos, llevando rápidamente a la atención de la gerencia cualquier condición que pudiera interrumpir el trabajo, para que así se tomen acciones correctivas con prontitud. Ejemplos de temas que deben ser reportados incluyen: errores inexplicables al escribir una unidad de disco duro, archivos extraviados en un computador personal, equipo de computación robado, extintores de incendios que no se recargan y otros peligros potenciales. Esta política requiere que los trabajadores actúen responsablemente, al menos en el sentido de notar el problema. Es preferible tener muchos ojos y no pocos para darse cuenta de estas cosas.

Políticas Relacionadas: “Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio” y “Sistema de Alerta de Seguridad Informática”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Reportes Centralizados de Problemas

Política: Todas las vulnerabilidades conocidas e infracciones sospechadas o conocidas deben ser comunicadas de manera expedita y confidencial al departamento de

Seguridad Informática, y las divulgaciones no autorizadas de información de la Empresa X deben adicionalmente ser reportadas al Propietario correspondiente de la información.

Comentario: Esta política tiene la intención de establecer un departamento centralizado de Seguridad Informática como el punto focal de todos los reportes de vulnerabilidades e infracciones. En muchas organizaciones, estos reportes sólo llegan a los niveles bajos de gerencia y nunca encuentran el camino de regreso a un grupo centralizado. A menos que exista un grupo centralizado de reportes, no existirán históricos recopilados de pérdidas, no se conducirán análisis de pérdidas y no se tomarán decisiones relativas a toda la organización. La centralización de reportes es también útil para la movilización de un equipo de respuesta ante emergencias de computación, un plan de contingencia de toda la organización, y otros recursos importantes de defensa. La política también ayuda porque elimina la preocupación del denunciante acerca de pasar por encima de un jefe. Sin una política como ésta, la gerencia local se indisponer porque los reportes de problemas los hacen ver mal y no pueden evitar que el proceso de reporte llegue hasta la alta gerencia. La política también sirve de ayuda porque indica lo que debe ser comunicado y a quién. Esta política asume que ya existe una política separada que define al Propietario de la información.

Políticas Relacionadas: “Daño y Pérdida de Sistemas Fuera de Sede” y “Conflictos Legales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Discusiones Sobre Debilidades y Vulnerabilidades en la Seguridad

Política: Los trabajadores que descubran debilidades o vulnerabilidades en las medidas de seguridad utilizadas por la Empresa X, no deben discutirlas con personas ajenas a la gerencia de Seguridad Informática, la gerencia de Auditoría Interna o los investigadores designados por uno de estos dos gerentes.

Comentario: Esta política evita los rumores sobre las debilidades y vulnerabilidades asociadas con las medidas de seguridad informática utilizadas por la organización que adopte esta política. Aquellos que descubren debilidades o vulnerabilidades frecuentemente quieren compartir sus observaciones para recibir algún reconocimiento. Esta política explícitamente prohíbe esa tendencia porque tiene un alto riesgo de

estimular a otras personas a explotar las debilidades y vulnerabilidades que se han descubierto. Las discusiones extensas de estos asuntos erosionan la confianza del trabajador en la habilidad de la organización de mantener el control sobre sus operaciones internas y también aumentan el riesgo de que esta información pase a grupos externos tales como periodistas, competidores y ex-empleados disgustados.

Políticas Relacionadas:“Reportes de Brechas de Seguridad a Terceros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

5. Reporte de Vulnerabilidades en la Seguridad

Política: Cuando se descubra una vulnerabilidad nueva y seria en la seguridad de los sistemas informáticos, asociada con el hardware o software de un proveedor en particular, la vulnerabilidad debe ser inmediatamente reportada al foro público apropiado para lograr su diseminación pública.

Comentario:La política está basada en la teoría de que si el problema es comunicado al proveedor de manera callada y confidencial, entonces hay poca intención por

arreglar el problema con prontitud. Aquéllos que adoptan esta política creen que es a través de la vergüenza pública que se corregiría la vulnerabilidad. Aquéllos que adoptan esta política también creen que los administradores de sistemas y otros, necesitan los detalles sobre un nuevo problema para que entiendan cómo pueden proteger mejor sus sistemas. Desafortunadamente, muchos administradores de sistemas no tienen el tiempo ni el adiestramiento necesarios para efectuar correcciones de vulnerabilidades que han sido públicamente anunciadas, y que pueden ser utilizadas hasta el momento en que el proveedor ponga en circulación sus propias correcciones. Un gran problema con esta política es que puede alertar a la comunidad de hackers clandestinos, lo que puede llevar al poco tiempo a la utilización de programas públicamente disponibles que automatizan el ataque. Como soporte de esta política, algunos argumentan que la comunidad de hackers probablemente ya está en conocimiento de ello y que mantenerlo callado sólo permite que la comunidad de hackers continúe abusando de la vulnerabilidad en secreto.

Políticas Relacionadas:“Divulgación de Vulnerabilidades” y “Reportes Externos de Violaciones”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

6.03.03 Reporte de Fallas en el Software

1. Notificación de Falla en los Controles de la Integridad

Política: Si fallan los controles que aseguran la integridad de la información, si se sospecha de fallas en estos controles o si los controles no están disponibles, la gerencia debe ser notificada de estos hechos cada vez que se obtenga la información correspondiente.

Comentario:La intención de esto es lograr la completa divulgación de la naturaleza de la información utilizada para la toma de decisiones. Si se sospecha de cierta información o si se pudiese sospechar, la gerencia debe ser notificada. Esta política requiere que la gerencia sea notificada, en vez de que la información se suprima con la esperanza de que nadie la descubra. Esta política requiere que las malas noticias se difundan, en lugar de permitir tácitamente que se supriman. Particularmente en organizaciones grandes hay una tendencia a suprimir las malas noticias a medida que la información sube en la jerarquía gerencial.

Políticas Relacionadas:“Responsabilidad en la Seguridad Informática”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

2. Divulgación de Vulnerabilidades

Política: Los trabajadores deben otorgar al proveedor un tiempo razonable para arreglar cualquier problema serio de vulnerabilidad en el sistema descubierto en la Empresa X, antes de hacer pública cualquier información sobre dicho problema.

Comentario:Esta política evita situaciones desafortunadas en las que empresas, y a veces individuos, anuncian haber encontrado una seria vulnerabilidad para la cual no hay arreglo. El actuar de esta manera permite a los hackers, a los espías industriales, ex-empleados disgustados y otros, explotar la información en la forma que deseen. Lo responsable es darle al proveedor tiempo

para diseñar una solución y anunciar la disponibilidad de dicha solución. Sin embargo, la presión por parecer un experto y las presiones por recibir la atención del mercado antes de que alguien descubra el mismo problema, ha causado que muchas organizaciones anuncien vulnerabilidades antes de que el proveedor esté listo para suministrar una solución. Esta política deliberadamente no menciona un período de tiempo porque ello depende de la naturaleza del problema. La amenaza de publicación puede ser usada por los trabajadores de la Empresa X para obligar al proveedor involucrado a diseñar con prontitud una solución. Si el proveedor no lo hace en un tiempo oportuno, los trabajadores podrán anunciar el problema.

Políticas Relacionadas: “Reportes Centralizados de Problemas” y “Discusiones Sobre Debilidades y Vulnerabilidades en la Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Informe de Sospecha de Virus

Política: Los trabajadores que sospechen de la existencia de un virus en el computador y lo reporten al departamento de Seguridad Informática inmediatamente después de descubierto, no deben ser castigados a menos que el trabajador conscientemente haya causado la introducción del virus en los sistemas de la Empresa X.

Comentario: Esta política está dirigida a estimular el rápido reporte del virus, lo cual es esencial para limitar su crecimiento y contener las pérdidas subsiguientes. Un aspecto importante de la política es que si hay demora en reportar el problema se tomará la acción disciplinaria. Se usó la palabra "inmediatamente" en la política dado que sólo unos minutos pueden constituir una gran diferencia cuando se trata de la propagación de un virus. Si un trabajador ha diseñado un virus y lo suelta en los computadores de la Empresa X, esto debe ser una causa de acción disciplinaria, aun cuando el empleado informe con prontitud al departamento de Seguridad de Informática después que se le fue de las manos. La política puede ser ampliada para incluir gusanos,

caballos de Troya, y otros programas no autorizados que pueden significar un riesgo para los sistemas de la Empresa X.

Políticas Relacionadas: “Exploración del Software,” “Informes de Violaciones y Problemas,” y “Eradicación de Virus de Computadores”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Informe de Funcionamiento Incorrecto de Software

Política: Todo funcionamiento aparentemente incorrecto del software debe ser inmediatamente reportado a la gerencia de línea o al proveedor de servicios de sistemas informáticos.

Comentario: Esta política requiere que los usuarios noten y reporten cualquier software que aparentemente esté funcionando de manera diferente a la señalada en su documentación. Esto ayudará a descubrir caballos de Troya, virus, problemas de contabilidad, fraudes y otros problemas. La política indirectamente también estimula el mantenimiento de la documentación actual. Esta política puede ser ampliada para instruir a los usuarios a apagar el computador y desconectarlo de cualquier red a la cual estén conectados. Estas acciones ayudan a aislar el problema para minimizar daños adicionales. De igual forma, en una política como ésta, se instruye a los usuarios a no intentar una recuperación. En estos casos, los expertos deben efectuar el esfuerzo de recuperación. Esta política puede ser cambiada para exigir que el reporte se haga al departamento de Seguridad Informática. A medida que las organizaciones expanden la conectividad de sus redes, esta política se hace más importante, porque esta interconectividad puede suministrar nuevos caminos para la transmisión de virus, gusanos, caballos de Troya y otro software no autorizado.

Políticas Relacionadas: “Informe de Sospecha de Virus”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6.03.04 Aprendizaje de Incidentes

1. Análisis de Violaciones y Problemas

Política: El departamento de Seguridad Informática

debe preparar un análisis anual de los problemas y violaciones reportados en seguridad informática.

Comentario: Esta política requiere que el departamento de Seguridad Informática prepare un reporte del estado de pérdidas actuales y problemas encontrados. Tal análisis de pérdidas ayuda al momento de efectuar evaluaciones de riesgos, cuando se preparan evaluaciones de desempeño y también cuando se preparan presupuestos y planes de proyectos para el año siguiente. Esta política puede ayudar a establecer y mantener una vía normal de comunicación con la alta gerencia. Nótese que la metodología para efectuar tal análisis no se menciona, con el fin de darle flexibilidad a Seguridad Informática para cambiar su enfoque a

medida que éste se torna más sofisticado. La política puede ser ampliada para incluir la mención del suministro de un reporte escrito al jefe oficial de información, al jefe ejecutivo, o al comité de auditoría de la junta directiva.

Políticas Relacionadas: “Investigación de Delito Computarizado” y “Retención de la Información Sobre Violaciones y Problemas de Seguridad”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

6.03.05 Proceso Disciplinario

1. Consecuencias de Incumplimiento

Política: El incumplimiento de las políticas, normas o procedimientos de seguridad informática es causa de acciones disciplinarias que pueden llegar hasta el despido.

Comentario: Esta política enfatiza la importancia de la seguridad informática y que se pueden producir acciones disciplinarias contundentes si el trabajador no la cumple. La política también tiene la intención de suministrar a la gerencia una justificación por sus acciones si un trabajador llegase a argumentar que una medida disciplinaria es innecesaria o injusta. Algunas organizaciones quieren especificar algunas de las posibles acciones disciplinarias, como por ejemplo, suspensión sin paga, descenso en su categoría, o transferencia a otro trabajo menos confidencial. La mayoría de las veces, sin embargo, esta especificación no será necesaria, ya que las políticas de recursos humanos tomarán en cuenta las posibles acciones de la gerencia de acuerdo con un proceso disciplinario normalizado.

Políticas Relacionadas: “Consecuencias de las Violaciones”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Consecuencias de las Violaciones

Política: Suponiendo que las acciones son incidentales o accidentales, la primera infracción de seguridad informática debe generar una advertencia, la segunda vez por el mismo motivo debe generar una carta para incluirla en el archivo personal del trabajador correspondiente; la tercera infracción por el mismo asunto implica suspensión por cinco días sin paga; la cuarta vez por el mismo motivo deben ser despedidos y las infracciones premeditadas o intencionales, independientemente de la cantidad, deben generar una acción disciplinaria que puede incluir el despido inmediato.

Comentario: Las leyes en muchas jurisdicciones requieren que un trabajador sea notificado antes de recibir una acción disciplinaria severa o el despido. Esta política tiene la intención de suministrar un creciente grupo de acciones disciplinarias severas que reflejen las infracciones de seguridad informática. En muchas organizaciones será innecesario especificar tales pasos porque una política más general de recursos humanos ya ha cubierto estos asuntos. Los detalles se incluyen en este manual para las organizaciones que no tienen una progresión documentada de crecientes medidas severas disciplinarias. Las medidas disciplinarias especificadas aquí pueden ser reemplazadas con otras que sean más comunes en otras organizaciones, industrias o países.

Políticas Relacionadas: “Consecuencias de Incumplimiento”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

3. Pérdida de Opciones en Valores

Política: Si el receptor de opciones en valores divulga información interna de la Empresa X a personas no autorizadas, dichas opciones deben ser revocadas.

Comentario: A través de esta política se envía un mensaje acerca de la necesidad de mantener en secreto la información confidencial. A veces, la gerencia se olvida de la seguridad informática, pensando que todo está bien. Esta política es especialmente importante en compañías que pronto o recientemente transan valores en bolsa a través de una oferta pública inicial. La política es más potente mientras mayor sea el porcentaje de ingresos que derive un empleado de sus valores. La alta gerencia generalmente presta mayor atención a esta política porque frecuentemente ellos obtienen un alto porcentaje de ingreso de las opciones en valores. La política puede ser modificada para incluir otras infracciones de seguridad informática, no sólo divulgaciones no autorizadas.

Políticas Relacionadas: “Consecuencias de Incumplimiento” y “Despidos Inmediatos”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

4. Despidos Inmediatos

Política: A menos que se obtenga un permiso especial de un vicepresidente ejecutivo, todos los trabajadores que hayan robado propiedad de la Empresa X, o que actúen con insubordinación, o que hayan sido convictos de un delito, deben ser despedidos inmediatamente, acompañados mientras recogen sus pertenencias personales y escoltados fuera de las instalaciones de la Empresa X.

Comentario: Esta política requiere que la gerencia despida a los trabajadores que han demostrado ser una amenaza justificada para la seguridad de la organización o de sus trabajadores. Por ejemplo, si un empleado ha sido condenado por asesinato mientras está empleado en la Empresa X, su presencia en la oficina puede constituir un riesgo innecesario. Esta política le da a la gerencia flexibilidad en cuanto a determinar mejores opciones además del despido, tal como la suspensión sin paga en caso de que tenga la intención de recuperar al empleado. Repuestas más leves a estos serios problemas siempre pueden ser decididos o aprobados por un vicepresidente ejecutivo. Debido a que es un especial riesgo el tener allí a estos individuos, particularmente si están en una

posición de confianza en computación, se requiere la consideración de la alta gerencia para permitir su presencia. Las circunstancias específicas que llevan al despido inmediato se pueden cambiar para satisfacer la preferencia de la gerencia de la Empresa X. Documentar estas acciones en una política reducirá la probabilidad de que un trabajador despedido pueda argumentar en un juicio que el despido fue injustificado e ilegal.

Políticas Relacionadas: “Consecuencias de las Violaciones”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

5. Despidos Bajo Coacción

Política: Los computadores personales utilizados por el trabajador despedido bajo coacción deben ser inmediatamente aislados tanto de Internet como de la red interna de la Empresa X, se deben reformatear sus discos duros y se debe reinstalar el sistema correspondiente de software.

Comentario: Esta política impide que los trabajadores despedidos en circunstancias incómodas puedan vengarse haciendo daño a su ex-empleador. Más allá de la acostumbrada cancelación de sus privilegios de acceso, esta política dice que sus computadores deben ser aislados. Este aislamiento evita que el software que estos trabajadores escribieron y almacenaron en sus computadores, pueda hacer daño a los sistemas de la Empresa X. La ejecución de este software puede no requerir los privilegios que el trabajador tenía para hacer serios daños. La razón por la cual los discos duros deben ser formateados, es porque el software puede estar esperando hasta que sea reconnected a la red. Reformatear el disco duro y reinstalar todo el software del sistema debería ser suficiente. El procedimiento subrayado en esta política ayuda a evitar que el empleado despedido pueda evadir los controles de seguridad y acceder al sistema otra vez. Aunque esta política puede restringirse sólo al personal técnico, hay muchos usuarios finales sofisticados, capaces de codificar el software discutido en esta política.

Políticas Relacionadas: “Base de Datos Centralizada de Controles de Acceso” y “Manejo de Despidos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

7 SEGURIDAD FÍSICA Y AMBIENTAL

7.01 Areas Seguras

7.01.01 Perímetro de Seguridad Física

1. Acceso Físico para Terceros

Política: El acceso de visitantes o terceros a las oficinas de la Empresa X, o salones de computación y otras áreas de trabajo que contengan información confidencial, debe ser controlado por guardias, recepcionistas u otro personal.

Comentario: Esta política requiere que el personal autorizado se involucre en el proceso de determinar si los visitantes o terceros pueden estar en las áreas que contienen información sensible. El acceso sin control a esas áreas puede acarrear espionaje industrial, estafas, robo de equipo y otros problemas. Esta política define una manera de llevar a cabo una estrategia conocida como "control del perímetro", un procedimiento clásico utilizado en la época medieval. Para hacer cumplir esta política, la entrada de empleados puede contar con torniquetes u otros mecanismos para garantizar que sólo los trabajadores autorizados, utilizando un dispositivo u otro mecanismo de control de acceso, puedan entrar. El alcance de la política puede ser ampliado para incluir información crítica o valiosa.

Políticas Relacionadas: ["Clasificación de Datos en Cuatro Categorías,"](#) ["Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,"](#) y ["Control de Acceso Físico a la Información Sensible"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Plan de Seguridad Física

Política: Todo centro de datos de la Empresa X debe tener un plan de seguridad física que debe ser revisado y actualizado anualmente por el gerente a cargo de las instalaciones.

Comentario: Esta política explícitamente asigna la responsabilidad para el desarrollo y actualización de los planes de seguridad física del centro de datos. Esta política establece claramente que la seguridad física es una línea de responsabilidad gerencial, no una responsabilidad del departamento de personal. Esto quiere decir que la seguridad física debe ser tratada dentro del

curso ordinario de las operaciones del centro de datos, no exclusivamente por un grupo especial. Un grupo técnico especial, normalmente llamado departamento de Seguridad Física, está generalmente disponible para consultas y asistencia. En la mayoría de los casos, el gerente a cargo del centro de datos no prepara el plan, sino alguna otra persona que reporta al gerente. Algunas organizaciones pueden querer incluir palabras en la política que indiquen que este plan estará sujeto a revisiones periódicas por Auditoría Interna. Esta declaración puede ser omitida de la política como se ha hecho aquí. Debe haber una buena seguridad física si se quiere tener una buena seguridad informática. Por ejemplo, si cualquier persona de la calle puede entrar en un centro de datos, iniciar un computador y después cargar su propia versión de un sistema operativo, casi todo, cuando no todo, el buen trabajo en el área de seguridad informática será nulo de toda nulidad.

Políticas Relacionadas: ["Lógica Crítica de Negocios"](#) y ["Planes de Respuesta Ante Emergencias Computacionales"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

3. Ubicación del Centro de Computación y Comunicaciones

Política: Los computadores multiusuario y las instalaciones de comunicaciones deben estar ubicados más arriba de un primer piso, alejados de cocinas y en una ubicación separada de las paredes exteriores del edificio mediante una pared interna, en un salón sin ventanas.

Comentario: Esta política suministra orientación para aquéllos que tienen la responsabilidad de ubicar la instalación de computadores multiusuario dentro de un edificio. Muchos de los gerentes responsables de ubicar centros de computación no consideran estos asuntos y los problemas surgen una vez completada la instalación. Por lo menos el conocimiento de estos problemas ayudará al gerente a instalar otros controles que reduzcan o eliminen las pérdidas, aun cuando la ubicación del centro de computación no se modifique.

Políticas Relacionadas: “Posiciones de las Pantallas de los Computadores” y “Ubicaciones de Centros de Computación”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4. Resistencia al Fuego de Centros de Computación

Política: Debe haber paredes cortafuego alrededor de los centros de computación, las cuales deben ser resistentes al fuego por lo menos durante una hora y todas las salidas de dichas paredes, tales como las puertas y los ductos de ventilación, deben cerrarse automáticamente y ser resistentes al fuego por lo menos durante una hora.

Comentario: Esta política claramente especifica un mínimo aceptable de resistencia al fuego en la construcción de centros de computación. Lo mismo puede aplicarse a los centros de comunicación, tales como el centro de control de la red. Las aperturas, como los ductos de ventilación, deben cerrarse automáticamente al igual que las puertas, si se activa la alarma de incendio. El fuego es la causa más común de desastres en centros de computación y frecuentemente el incendio comienza en áreas adyacentes y después se extiende al centro de computación. Si la construcción se realiza con materiales resistentes al fuego, entonces aumentan las probabilidades de que el incendio sea controlado antes de causar mayores daños.

Políticas Relacionadas: “Fumar, Comer y Beber”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Solidez de las Puertas de Centros de Computación

Política: Los salones de los centros de computación deben estar equipados con puertas antimotines, puertas resistentes al fuego y cualquier otra puerta resistente a entradas forzadas.

Comentario: La intención de esta política es garantizar que las puertas de los centros de computación suministrarán una protección adecuada al costoso equipo que en ellos se encuentran. En muchas oficinas, no existen puertas cerradas a los salones de computación, especialmente donde están ubicados sistemas pequeños, como los servidores de la red de área local. La política puede

ser extendida para exigir que todas las puertas abran automáticamente al activarse la alarma de incendio, o cuando existe una necesidad urgente por salir. La política puede ser expandida con el fin de incluir los centros de comunicaciones, tales como los centros de administración de la red.

Políticas Relacionadas: “Resistencia al Fuego de Centros de Computación” y “Cierre de Puertas en Centros de Computación”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Cierre de Puertas en Centros de Computación

Política: Los salones de las instalaciones de computación deben estar equipados con puertas que se cierren inmediatamente después de ser abiertas, y con una alarma sonora que se dispare cuando han estado abiertas más allá de un cierto tiempo.

Comentario: Los requerimientos manifestados en esta política evitan que las personas dejen las puertas abiertas para que otros puedan entrar. Dicho tipo de puertas ayuda a que el control de acceso físico establecido por la gerencia realmente se utilice mientras se registran entradas y salidas. Estas puertas han demostrado ser efectivas en lo que se refiere a obligar a las personas a usar el sistema de control de acceso físico. La política puede ser ampliada para incluir las instalaciones de comunicaciones, tales como los centros de administración de redes. Si las personas están dejando las puertas abiertas, deben investigarse las razones. Por ejemplo, si el aire acondicionado no está funcionando bien en la época de verano, hay que mantener la puerta abierta.

Políticas Relacionadas: “Resistencia al Fuego de Centros de Computación” y “Solidez de las Puertas de Centros de Computación”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

7. Puertas Adicionales de Acceso al Centro de Computación

Política: Todas las puertas adicionales de un centro de computación deben estar equipadas con barras de choque que activen una alarma al abrirse.

Comentario: Esta política especifica las normas para la construcción de centros de computación incluyendo los centros de operación de redes. Establece que todas las puertas adicionales a la principal deben tener barras de choque. Las barras de choque activan una alarma sonora, aunque la electricidad al centro esté cortada. De esta manera, se alerta al personal de guardia que una puerta se ha abierto y que posiblemente una persona no autorizada está obteniendo acceso a un área restringida.

7.01.02 Controles Físicos de las Entradas

1. Control de Acceso Físico a la Información Sensible

Política: El acceso a toda oficina, sala de computación y área de trabajo que contenga información sensible debe ser físicamente restringido para limitar el acceso a aquéllos que necesitan la información.

Comentario: Esta política requiere que la gerencia local restrinja el acceso a las áreas donde existe información sensible. La tecnología específica requerida para manejar esta información, deliberadamente no se ha mencionado. La información puede estar en una copia impresa, ser discutida por teléfono o en los planos de construcción del edificio. La gerencia local debe consultar a los especialistas de seguridad interna para que determinen qué tipo de tecnología de control de acceso debe ser usada. Las circunstancias varían tanto entre los sitios de trabajo, que pudiera no ser conveniente requerir que todas las oficinas usen una determinada tecnología de control de acceso, particularmente en compañías multinacionales que se enfrentan a requerimientos y costumbres locales muy diferentes. Desde un punto de vista de contención de costos y de la normalización de ciertas tecnologías para el control físico de acceso, pueden preferirse las tarjetas magnéticas. Esta política es particularmente importante para ambientes de computación con computadores personales, redes de área local, estaciones de trabajo y sistemas cliente-servidor, porque los controles lógicos de acceso en tales sistemas son frecuentemente imprecisos o están ausentes. El alcance de la política puede ser ampliado para incluir información "crítica o valiosa".

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#),” “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#),” y “[Acceso Físico de Trabajadores Cesados](#)”

Política Dirigida a: Gerencia

La alarma puede también avisar a otros que puede haber un incendio o cualquier otro problema que necesita atención inmediata.

Políticas Relacionadas: “[Control de Acceso Físico a la Información Sensible](#)” y “[Áreas Desatendidas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

Ambientes de Seguridad: Todos

2. Cierre de Oficinas Personales

Política: Todos los trabajadores con oficinas propias separadas deben cerrar sus puertas con llave cuando las oficinas no estén en uso.

Comentario: Esta política hace que los trabajadores utilicen los seguros de las cerraduras de las puertas de su oficina, las cuales normalmente son equipo normal en edificios de oficinas. Con frecuencia, esta medida básica de control es ignorada y después de horas de oficinas se producen divulgaciones no autorizadas de información sensible o cuando el área de trabajo está desatendida. La política debe ser acompañada por un fuerte sistema de administración física de las llaves, que permita a la gerencia o a las secretarías entrar en caso de emergencia mediante llaves maestras. Esta política asume que las oficinas tienen cerramiento total. Esta política no es apropiada si las oficinas son cubículos u otro tipo de oficina sólo parcialmente cerradas. Aunque esta política pudiera parecer básica, obvia y quizás no tan importante como para estar en un documento de seguridad informática, sí es relevante aclarar estas instrucciones por escrito si se desea un cumplimiento consistente.

Políticas Relacionadas: “[Control de Acceso Físico a la Información Sensible](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Distintivos de Identificación

Política: Mientras se encuentren dentro de las instalaciones o edificios seguros de la Empresa X, las personas deben portar sus dispositivos de identificación de tal manera que la foto y la información sean claramente visibles.

Comentario: El propósito de esta política es notificar a todos los trabajadores la obligación de portar sus distintivos en sitio visible. Esto permitirá a los guardias y otros trabajadores determinar si la persona puede tener acceso a cierta área. La política permitirá que los trabajadores se den cuenta fácilmente si alguien está usando un distintivo prestado o robado. Esta política asume que los distintivos tienen fotos, pero la referencia a las fotos puede ser omitida si no es el caso. Esta política funciona bien cuando se trata de localizar personas no autorizadas en áreas restringidas. Si solamente ciertas áreas son restringidas a través del uso de distintivos, la política pudiera aplicarse sólo a las áreas restringidas en vez de a todos los edificios e instalaciones de la Empresa X. A algunos trabajadores no les gusta tener la foto en el distintivo, pues piensan, por ejemplo, que no es halagador y estas personas pueden desear esconder sus distintivos, pero este comportamiento no es aceptable en función de esta política. Estas personas deben ser invitadas a tomarse una nueva foto para un nuevo distintivo y así se sentirán más cómodas usándolo.

Políticas Relacionadas: “Personas Sin Distintivos de Identificación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Distintivos Temporales

Política: Los trabajadores que hayan olvidado traer sus distintivos de identificación deben obtener un distintivo temporal válido por un día, a cambio de su licencia de conducir o cualquier otra identificación con foto.

Comentario: El propósito de esta política es enfatizar que todo trabajador debe portar un distintivo de identificación, aun cuando haya olvidado traer el original. Si los trabajadores constantemente olvidan traer su distintivo, los registros del departamento de Seguridad mostrarán la cantidad de veces que les han otorgado distintivos temporales. Si el número de distintivos temporales de alguien en particular es excesivo, debe notificarse al gerente de esa persona. Las distintivos temporales deben expirar al final del día, en el caso de los visitantes que olviden regresarlos y también para inducir a los trabajadores a traer su distintivo normal el día siguiente. Para demostrar fácilmente su expiración, algunos tipos de distintivos pierden el color después de cierto tiempo. La identificación es necesaria para demostrar que una persona es quien dice ser, lo cual evitara que terceros las utilicen alegando ser trabajadores que olvidaron traer su distintivo. Un sistema de

distintivos temporales implica que hay una base de datos en el computador que contiene los privilegios de entrada y las fotos de los empleados, y que estos privilegios pueden imprimirse fácilmente en un distintivo nuevo. Si éste no es el caso, ello significa que esta política y sus procedimientos no son prácticos. La política se aplica a todos los trabajadores.

Políticas Relacionadas: “Iniciación de Transacciones en Computadores” y “Reportes de Distintivos de Identificación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Acceso Controlado con Distintivos

Política: Toda persona debe presentar su distintivo al lector de distintivos antes de entrar por cualquier puerta controlada, dentro de las instalaciones de la Empresa X.

Comentario: Esta política tiene la intención de garantizar que en el registro de control de entradas se reflejan los individuos que realmente estaban presentes en el área y a la hora que se especifica. Frecuentemente un grupo de personas entran por una puerta controlada y sólo es registrado el primero de ellos. Esta práctica puede ser explotada por espías industriales, personal de organizaciones competidoras y otros que buscan entrar sin autorización a áreas que contienen información sensible. Los detalles de cómo se ejecuta esta política varían en función de la tecnología de control de entrada utilizada. Los torniquetes son ideales porque es muy difícil o imposible la entrada de dos personas a la vez. La política se refiere a “personas” en vez de “trabajadores”, porque algunas personas en el área son visitantes o proveedores. Esta política puede causar una acumulación de solicitudes de entrada justo antes de comenzar el horario de trabajo ya que muchas personas convergen en las puertas controladas al mismo tiempo.

Políticas Relacionadas: “Distintivos de Acceso Compartidos”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Distintivos de Acceso Compartidos

Política: Los trabajadores no deben permitir a personas desconocidas o no autorizadas pasar por puertas, rejas u otras entradas a áreas restringidas al mismo tiempo que las personas autorizadas.

Comentario: Esta política intenta evitar que personas no autorizadas entren después de personas autorizadas a las áreas controladas; por ejemplo, utilizando la llave o tarjeta de una persona autorizada para abrir la puerta. Si se utilizan torniquetes o controles parecidos, esta política es menos importante. La política puede ser ampliada para requerir que los trabajadores autorizados refieran a las personas desconocidas o no autorizadas a una recepcionista o estación de vigilancia. En la política el término "áreas restringidas" puede ser reemplazado por un área específica, tal como "centro de computación".

Políticas Relacionadas: "[Personas Sin Distintivos de Identificación](#)" y "[Acceso Controlado con Distintivos](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Entradas Individuales

Política: Todas las entradas de tráfico peatonal a todos los centros de datos de la Empresa X deben tener mecanismos de trampas humanas.

Comentario: Esta política impide que personas mantengan la puerta abierta para otros, y por ende permitir que personas no autorizadas entren al centro de datos. Al requerir que las personas pasen a través de puertas controladas, uno por uno, la organización impide que se entre en grupos. A pesar de que un torniquete puede ser utilizado para este propósito, la trampa humana individual suministra una medida de control adicional donde un intruso puede quedar encerrado hasta que llegue el personal de seguridad. Una trampa humana también puede ser configurada para que las personas salgan del área individualmente. Las instalaciones de una organización externa también pueden ser consideradas para este tipo de controles físicos, así como los centros de datos de la Empresa X cubiertos por esta política. La palabra "pedestre" fue incluida en esta política para distinguir estas entradas de las rampas de descarga, las cuales no pueden ser controladas con trampas humanas.

Políticas Relacionadas: "[Acceso Físico para Terceros](#)" y "[Etiquetas Anti-Robo](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

8. Intentos No Autorizados de Acceso Físico

Política: Los trabajadores no deben intentar entrar en áreas restringidas de la Empresa X para las que no han sido autorizados.

Comentario: Esta política notifica a los trabajadores que no deben intentar inhabilitar los controles físicos de entrada. Si los trabajadores necesitan entrar a cierta área, deben acudir a los canales apropiados de autorización en vez de tomar las cosas en sus propias manos. Puede que existan emergencias y desastres donde esta política no se pueda aplicar. En estas circunstancias, los trabajadores deben hacer lo que tienen que hacer y dar explicaciones después. Los sistemas de control registrarán intentos de entrada a áreas donde el individuo no tenga permiso de entrada. Esta política establece las bases para acciones disciplinarias cuando se han cometido varios intentos de entrada a un área no autorizada.

Políticas Relacionadas: "[Prueba de los Controles del Sistema Informático](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Inspección de Bolsos

Política: Todos los maletines, maletas, carteras y demás equipajes deben ser abiertos para que los guardias de la Empresa X los revisen al momento de salir las personas de las instalaciones.

Comentario: El objetivo de esta política conservadora es disuadir a las personas de llevarse información sensible o valiosa. La política es un gesto disuasivo, no un método infalible de evitar robos de información sensible y valiosa. Esta política tiene una gran falla. Es probable que los guardias no distingan la información sensible o valiosa. Por ejemplo, un guardia de seguridad no se va a tomar el tiempo de revisar la información contenida en un disquete que alguien lleve en su maletín. Aún cuando la información sensible y valiosa puede estar impresa en un papel especial de color llamativo, o etiquetada con marcadores magnéticos que activen una alarma cuando son removidos del edificio, estos procedimientos son relativamente ineficaces contra un ladrón decidido. Esta política es más efectiva cuando intenta disuadir y ocasionalmente descubrir un robo de equipo o material de computación.

Políticas Relacionadas: "[Pases de Propiedad](#)" e "[Información Secreta Fuera de Oficinas](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

10. Registros del Sistema de Control de Acceso

Política: El departamento de Seguridad debe mantener registros de las personas que están y han estado dentro de los edificios de la Empresa X, y guardar esta información en sitio seguro por lo menos durante tres meses.

Comentario: El propósito de esta política es registrar la información sobre quiénes entran y salen de un edificio que contenga información sensible, crítica o valiosa. Esta información es muy importante cuando los sistemas de control de acceso físico están combinados con un sistema de control de acceso computarizado. Por ejemplo, si un identificador de usuario se utilizó para cometer un fraude desde una ubicación dentro del edificio con control de acceso, pero el individuo que está autorizado para usar esa identificación, no estaba presente en ese momento, se demostraría que una persona no autorizada estaba usando el identificador de usuario. El saber quién está en un edificio es muy importante en caso de fuego, amenaza de bomba, o cualquier otra emergencia o desastre. Si se llevan registros de entradas y salidas, esto puede funcionar como un disuasivo contra acciones no autorizadas, como el robo de computadores. Tales registros también pueden ser importantes para demostrar que ciertas tarjetas de tiempo son fraudulentas. El mantenimiento de tales registros, también ayuda con el cumplimiento de las políticas, permitiendo que sólo aquéllos con necesidad de conocer puedan tener acceso a ciertas áreas.

Políticas Relacionadas: “[Período de Retención de Registros](#)” y “[Reportes de Distintivos de Identificación](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Acceso Físico de Trabajadores Cesados

Política: Cuando el trabajador finaliza su relación de trabajo con la Empresa X, todos los códigos de seguridad para el acceso físico conocidos o disponibles al trabajador, deben ser desactivados o cambiados.

Comentario: Esta política pretende limitar el acceso continuado de trabajadores cesados. La política está redactada de manera general con el propósito de incluir

códigos compartidos como números de combinación de la puerta principal y códigos individuales, tales como los números de identificación grabados en cinta magnética en un distintivo. Esta política evita la confusión sobre la identificación de la persona que está utilizando un código de acceso. La política también puede evitar que un trabajador cesado use una copia del mecanismo de acceso para entrar sin autorización a las áreas de trabajo de la Empresa X. Este último objetivo es particularmente importante si el trabajador está descontento. La política hace mención de “códigos de acceso conocidos por el trabajador”, pero pudiera ser cambiado por “códigos de acceso conocidos o disponibles al trabajador”. Este cambio sería necesario si los códigos estuviesen codificados en una tarjeta inteligente, pero en el estricto sentido de la palabra, sin el conocimiento del trabajador. La distribución de esta política normalmente está restringida al personal de los departamentos de Seguridad Informática y Seguridad Física.

Políticas Relacionadas: “[Separación de Actividades y Datos](#),” “[Devolución de Propiedad al Cesar Empleo](#),” “[Transferencias de Trabajadores](#),” e “[Informe de Cambios en Situación de Empleados](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Acceso de Trabajadores Cesados a Areas Restringidas

Política: Cuando un trabajador termina su relación de trabajo con la Empresa X, todos los derechos de acceso a las áreas restringidas de la Empresa X deben ser revocados inmediatamente.

Comentario: Esta política garantiza que los trabajadores que hayan terminado su relación de trabajo con una organización, no podrán entrar en las oficinas u otras áreas controladas, tales como la planta de manufactura. Las políticas del departamento de Recursos Humanos deben informar cuándo se revocarán los derechos de acceso. Esta política apoya la seguridad informática porque si una organización no puede controlar quién está dentro de un área restringida, tendrá muchos problemas restringiendo el acceso a la información restringida. Esta política está redactada para la gerencia, que con frecuencia debe manejar el proceso de cese laboral.

Políticas Relacionadas: “[Acceso Físico de Trabajadores Cesados](#)” y “[Restricción de Privilegios — Necesidad de Conocer](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

13. Lista de Otorgantes de Acceso Físico

Política: La lista de gerentes autorizados para otorgar permiso de acceso a las instalaciones de la Empresa X se debe mantener al día y debe ser revisada periódicamente por los gerentes superiores que hayan delegado esa autoridad al gerente correspondiente.

Comentario: Esta política establece una clara jerarquía que muestra la delegación de autoridad para otorgar acceso físico. Los gerentes mencionados en el primer enunciado son los que autorizan rutinariamente a ciertos trabajadores el acceso a áreas restringidas. Los "gerentes superiores" mencionados en la segunda parte son los que deciden cuáles gerentes harán las decisiones del día a día. La existencia de una clara y actualizada delegación de autoridad evitará que los gerentes que ya no estén autorizados, o removidos, transferidos o despedidos, hagan mal uso de su autoridad. De igual manera la existencia de esta jerarquía enfoca la atención en los derechos correspondientes a otorgar a los distintos gerentes, ayudando con ello a garantizar que los derechos otorgados están acordes con la necesidad del negocio.

Políticas Relacionadas:“[Otorgamiento de Privilegios del Sistema](#),” “[Autorización para Transacciones de Producción](#),” y “[Reportes de Distintivos de Identificación](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

14. Reportes de Distintivos de Identificación

Política: Una lista mensual de todas las personas de cada departamento que actualmente tienen distintivos de identificación autorizados, debe ser enviada a los jefes de departamento para su revisión y el inicio de alguna acción correctiva.

Comentario: Esta política requiere la emisión y revisión de un reporte que refleje los distintivos autorizados actualmente. Esto identificará y eliminará los distintivos vencidos, cuyos privilegios aún no hayan sido revocados. Si personas no autorizadas entran a las instalaciones de Empresa X, la seguridad de la información que se encuentra en dicho sitio estará indebidamente en riesgo. El proceso de generar y revisar el reporte puede también utilizarse efectivamente con

identificadores de usuario, tarjetas de crédito telefónicas y otros mecanismos de acceso. Este reporte debe referirse a todos los trabajadores.

Políticas Relacionadas:“[Lista de Otorgantes de Acceso Físico](#),” “[Reautorización de los Privilegios de Acceso de Usuario](#),” y “[Acceso a la Información Secreta](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

15. Identificación de Visitantes

Política: Todos los visitantes de la Empresa X deben mostrar una identificación con foto y firmar un registro antes de entrar.

Comentario: Esta política requiere que todos los visitantes, incluyendo empleados de diferentes localidades, muestren su identificación comprobando quiénes son antes de entrar en las áreas restringidas. Esto desalentará a personas no autorizadas de hacerse pasar como autorizados. También ayudará a garantizar que el listado que muestra quién entró y salió del área restringida, es preciso y refleja la identidad real del individuo correspondiente. Si la organización considera que mostrar la identificación con foto no es conveniente, puede recortar la política, requiriendo sólo un proceso de firma. Si sólo el proceso de firma se utiliza para muchas personas, entonces el acceso puede ser restringido solamente a aquéllos que tenían cita. Todos los demás tendrán que mostrar identificación. La política puede ser modificada para requerir tanto firma a la entrada como firma a la salida, con fecha y hora en ambas. La ventaja de requerir firma a la salida es que en una emergencia como un incendio, la gerencia podrá fácilmente determinar quién estuvo, o está, en el edificio. Otro objetivo de esta política es que desanima a los empleados a traer a sus amigos o familiares a la oficina.

Políticas Relacionadas:“[Escolta de Visitantes](#),” “[Distintivos de Acceso Compartidos](#),” e “[Identificación Positiva para Uso del Sistema](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

16. Escolta de Visitantes

Política: Los visitantes a las oficinas de la Empresa X incluyendo, sin limitantes, clientes, ex-empleados, familiares de trabajadores, contratistas de reparación de

equipos, personal de correo de la compañía y policías, deben permanecer escoltados todo el tiempo por un trabajador autorizado.

Comentario: Esta política evita que personas no autorizadas entren a áreas controladas de información confidencial o privada mientras estén dentro de áreas controladas, como una oficina, por ejemplo, porque pueden leer un memo que esté encima de un escritorio de un trabajador. Si los visitantes son escoltados, sus acciones pueden ser supervisadas y evitada la divulgación. Esta política también evita el robo de propiedades de la oficina como módem y propiedad personal, como carteras. Esta política funciona mejor si los baños están ubicados cerca del área de recepción. Si los visitantes deben pasar a través de puertas controladas para ir a los baños, podrían entonces impedir la aplicación de la política de escolta porque un recepcionista o guardia no puede abandonar su puesto.

Políticas Relacionadas: “Distintivos de Acceso Compartidos,” “Supervisión de Terceros,” e “Identificación de Visitantes”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

17. Escoltas Obligatorios para Todos los Visitantes en Horas No Hábiles

Política: Los visitantes deben ser escoltados por un empleado autorizado por un gerente departamental, cuando se encuentren en las oficinas o instalaciones de la Empresa X fuera del horario normal del negocio.

Comentario: Esta política evita que los visitantes anden errantes por las oficinas e instalaciones fuera de las horas normales de trabajo, y quizás obteniendo información confidencial, robándose objetos valiosos, instalando conexiones de espionaje o efectuando cualquier actividad no autorizada. Fuera del horario normal de trabajo habrá menos personas en el sitio como para darse cuenta de que un visitante está haciendo algo sin autorización. Esta política también permite que los escoltas sean solamente empleados autorizados, evitando así que contratistas, consultores y temporales sean los escoltas. Esta política no evita entregas en una rampa de embarque, remodelación o reconstrucción de edificio y actividades similares. Sólo dicta que estas actividades deben ser ejecutadas en presencia de un empleado autorizado. Esta política permite que los visitantes se muevan libremente dentro de ciertas áreas durante horas normales de trabajo y mantiene alta la productividad del trabajador, porque la

escolta no es obligatoria durante esas horas. En organizaciones de alta seguridad, pueden utilizarse sistemas automáticos electrónicos de ubicación de visitantes, a través del uso de distintivos de proximidad, en lugar de un escolta.

Políticas Relacionadas: “Despidos Inmediatos” y “Visitantes sin Escolta”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

18. Supervisión de Terceros

Política: Los individuos que no sean empleados, contratistas o consultores autorizados deben estar bajo supervisión mientras estén dentro de áreas que contengan información sensible de la Empresa X.

Comentario: Esta política garantiza que terceros cuyas intenciones se desconocen no estarán solos en áreas que contengan información sensible. Si estas personas no son supervisadas, puede haber espionaje industrial, robo de equipos y otros problemas. Por ejemplo, por efecto de esta política, un técnico que se encuentre instalando una línea para suscriptores debería ser escoltado en su paso por áreas restringidas. Esta política puede ser ampliada para incluir información valiosa o crítica, no sólo la información sensible.

Políticas Relacionadas: “Escolta de Visitantes” y “Personas Sin Distintivos de Identificación”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

19. Personas Sin Distintivos de Identificación

Política: Los individuos que no porten distintivo de identificación de la Empresa X en sitio visible deben ser interrogados sobre el mismo, y si no pueden producirlo inmediatamente deben ser escoltados hasta la recepción.

Comentario: El propósito de esta política es asegurar que todos porten siempre su distintivo de identificación mientras se encuentren en áreas restringidas. De no hacerlo, no hay manera de saber quién está autorizado y quién no. La seguridad física es un componente esencial de la seguridad informática. Si una organización no puede controlar la presencia de las personas en áreas restringidas, será muy difícil o imposible controlar la seguridad informática. Algunas organizaciones querrán añadir otra oración a su política que establezca que si alguien está preocupado por su seguridad física después

del interrogatorio sobre su distintivo, una alternativa aceptable es dirigirse al departamento de Seguridad Física.

Políticas Relacionadas: “Visitantes sin Escolta” y “Distintivos Temporales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

20. Visitantes sin Escolta

Política: Cuando un trabajador se percate de la presencia de un visitante sin escolta dentro de las áreas restringidas de la Empresa X, debe interrogarlo acerca de su visita a dicha área, y luego escoltarlo hasta la recepción, hasta un guardia de seguridad o hasta la persona a quien viene a visitar.

Comentario: Esta política evita que personas no autorizadas permanezcan solas en áreas controladas donde se maneja información sensible, patentada o privada. También garantiza que sólo habrá personas autorizadas en las áreas restringidas. La política es aplicable a esos ambientes donde se requiere el uso de un distintivo y en oficinas más pequeñas donde todos se conocen sin necesidad de distintivos. Si esta política es muy rigurosa, podría a cambio pedir que los trabajadores le pregunten a los terceros si necesitan ayuda para encontrar la localidad que están buscando. Si los trabajadores se encuentran en una situación de peligro físico, pueden como alternativa llamar al departamento de Seguridad Física, en vez de confrontar ellos mismos a una persona extraña o amenazante en el área.

Políticas Relacionadas: “Distintivos de Acceso Compartidos,” “Escolta de Visitantes,” y “Distintivos de Identificación”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

21. Visitantes al Centro de Datos y al Departamento de Sistemas Informáticos

Política: Los visitantes que no tengan que efectuar reparaciones a equipos de la Empresa X, o que no necesiten estar dentro del Centro de Datos o el departamento de Sistemas Informáticos, no deben entrar en dichas áreas.

Comentario: Esta política evita que los visitantes conozcan secretos industriales, roben manuales que puedan ser utilizados para meterse en los sistemas informáticos, saboteen equipos, pongan bombas y efectúen otras actividades dañinas. A veces, para ejecutar este tipo de actividades es necesario el acceso. La política reconoce que ciertos visitantes, por ejemplo el personal de mantenimiento del representante de los computadores, deben tener acceso físico, y para estas personas puede emplearse una escolta continua. Todos los otros visitantes pueden mirar desde una ventana que abre al pasillo interno para tener una idea de lo que está sucediendo. Esta política puede impresionar a los visitantes, porque demuestra que la gerencia está interesada en la seguridad.

Políticas Relacionadas: “Visitantes sin Escolta” y “Escoltas Obligatorios para Todos los Visitantes en Horas No Hábiles”

Política Dirigida a: Todos

Ambientes de Seguridad: Altos

22. Acceso a Sistemas de Computación y Comunicación

Política: Los edificios que contengan sistemas de computadores o de comunicaciones de la Empresa X, deben estar protegidos con medidas de seguridad física que impidan el acceso a personas no autorizadas.

Comentario: Esta política garantiza que se tomarán medidas de seguridad para proteger los sistemas de computación y de comunicación. Esto evita el robo, el uso no autorizado de equipos y otros problemas de información relacionados con la seguridad. Esta política es relevante para computadores personales, estaciones de trabajo, redes de área local y sistemas cliente-servidor, aunque se aplica a todos los tipos de sistemas informáticos. La política es importante porque los computadores pequeños y los equipos de oficina normalmente están protegidos sólo por medidas de seguridad física. La política puede restringirse a aquellos sistemas informáticos que manejen información crítica o sensible.

Políticas Relacionadas: “Acceso Físico para Terceros” y “Seguridad de la Información Sensible”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

23. Aseguramiento de Actividades de Manejo de Información Sensible o Crítica

Política: Todas las actividades de manejo de información crítica o sensible de la Empresa X, se deben efectuar en áreas físicamente seguras y protegidas contra accesos no autorizados, interferencias y daños.

Comentario: Esta política garantiza que la gerencia tendrá controles adecuados sobre el acceso físico a los centros de computación, centros telefónicos, bóvedas de carpetas de archivos y otras localidades en donde se maneja información crítica o sensible. Las tecnologías a usarse no se mencionan en esta política debido a que la gerencia es quien debe tomar esta decisión. Las tecnologías de seguridad física deben estar elaboradas en función de la criticidad, el valor o la sensibilidad de la información y la ubicación del local.

Políticas Relacionadas: “Acceso a Sistemas de Computación y Comunicación” e “Información Secreta Fuerza de Oficinas”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

24. Acceso al Centro de Computación

Política: Los programadores, los usuarios y otros que no tengan necesidades de negocio para tal acceso, no deben entrar a los centros de computación.

Comentario: Esta política obliga a la separación de labores entre los operadores de computadores, los programadores y los usuarios. La política también reduce el congestionamiento y la confusión entre ellos. La política puede redactarse para que las palabras "centros de computación" se reemplacen por "centros de computación que contienen computadores personales, mainframes o sistemas de control de redes". Esta política no se aplica generalmente a sistemas departamentales, sistemas cliente-servidor o servidores de redes de área local, aunque podría hacerse.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,” “Separación de Tareas,” “Cambios en Producción,” y “Acceso a Librerías de Medios”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

25. Acceso del Personal al Centro de Computación

Política: El gerente de Operaciones Computarizadas debe mantener una lista revisada y actualizada por lo menos cada tres meses, del personal con acceso al centro de computación.

Comentario: Esta política establece un mecanismo mediante el cual la gerencia periódicamente revisará la lista del personal autorizado para entrar al centro de computación. En muchos negocios de computación, la gerencia no sabe quiénes tienen acceso a los centros de computación. Una revisión trimestral identificará a los trabajadores que ya no necesiten estar en el centro de computación y sus derechos de acceso pueden ser eliminados. Mientras algunas organizaciones prestan mucha atención a quién entra al edificio, pocas escudriñan quién puede entrar al centro de datos y las razones para otorgar dicho acceso.

Políticas Relacionadas: “Acceso al Centro de Computación” y “Acceso a Sistemas de Computación y Comunicación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

26. Acceso a Librerías de Medios

Política: Las bibliotecas de cintas magnéticas, discos y documentación deben estar restringidas a los trabajadores cuya responsabilidad exige su presencia en dichas áreas.

Comentario: Esta política restringe el acceso a áreas que contienen información sensible, valiosa o crítica y reduce la oportunidad de que dicha información se divulgue, manipule, borre o maneje de manera contraria a las intenciones de la gerencia. Esta política es una manifestación clara del principio de la separación de tareas. La referencia a "centro de computación" puede cambiarse a "centros de computación que contienen computadores personales, mainframes o sistemas de control de redes" o cualquier otra descripción organizacional específica.

Políticas Relacionadas: “Separación de Tareas” y “Acceso al Centro de Computación”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

27. Visitas a las Instalaciones de Computación

Política: No deben hacerse visitas públicas de las instalaciones de los principales centros de computación y comunicaciones.

Comentario: Esta política elimina las visitas públicas, las cuales pueden ser una cubierta por parte de los espías industriales, hackers, empleados disgustados y otros, listos para intentar algún daño para entrar a las áreas restringidas. Es sabido que individuos como éstos recogen información en el recorrido, la cual es un instrumento vital para comprometer los sistemas de control de acceso. Otros individuos han utilizado su proximidad al equipo de computación y comunicaciones mientras

están en el recorrido para sabotear sistemas. La política no prohíbe recorridos privados para empleados, consultores o contratistas con necesidad de conocer las instalaciones. Igualmente, esta política no prohíbe recorridos para la alta gerencia, inversores, accionistas y clientes importantes. Sin embargo, los recorridos educativos y turísticos están prohibidos.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#),” “[Señalización de Centros de Computación y Comunicaciones](#)” y “[Distintivos de Identificación](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7.01.03 Aseguramiento de Oficinas, Salones e Instalaciones

1. Limpieza Periódica para Evitar Equipos de Espionaje

Política: El gerente del departamento de Telecomunicaciones debe iniciar y supervisar barridos periódicos para detectar micrófonos ocultos no autorizados, interceptaciones y equipos de grabación en las oficinas y las instalaciones de la Empresa X, donde se discute, se almacena o se maneja información secreta.

Comentario: Esta política determina que se deben ejecutar barridos regulares para detectar micrófonos ocultos y aparatos interceptores. La política define quién debe iniciar y supervisar este esfuerzo. Mientras históricamente han sido parte de los establecimientos militares, estos barridos son ahora muy comunes en organizaciones comerciales. El negocio de espionaje industrial está creciendo y es ahora relativamente fácil implantar aparatos transmisores muy pequeños en teléfonos, debajo de mesas de conferencia y en otros lugares poco conspicuos. Tales barridos también buscan equipos de grabación en cassetas telefónicas. En muchos casos se necesitará un consultor externo con equipo especializado, debido a que la mayoría de las organizaciones no cuentan con personal suficientemente adiestrado.

Políticas Relacionadas: “[Conversaciones Telefónicas Sobre Información Sensible](#)” y “[Cifrado de Contraseñas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Aseguramiento de los Sistemas de Computación o Comunicación

Política: Todos los equipos multiusuario de computación y de comunicaciones deben estar ubicados en salones cerrados con llave.

Comentario: Sin importar cuán sofisticados sean los controles de acceso del software, si se obtiene el acceso físico a los servidores y equipos similares se pueden entonces vencer los controles de acceso del software. Por ejemplo, en muchos servidores de redes de área local, un simple proceso de reiniciación permitiría a la persona no autorizada controlar completamente la máquina y sus datos. La política alerta a la gerencia técnica en sitios remotos en el sentido de que todos los sistemas multiusuario deben ser ubicados en cuartos cerrados bajo llave. Los receptores típicos de esta política incluyen administradores de sistemas, gerentes de redes y otros responsables de equipos ubicados en sitios remotos. La política requiere que los conmutadores, los conmutadores telefónicos privados, los concentradores, los enrutadores, los cortafuegos y otros equipos de redes deben estar ubicados en un salón cerrado bajo llave. Esta política indirectamente promueve la ubicación de servidores y equipos similares en salones de computación con pisos falsos.

Políticas Relacionadas: “[Gabinetes Metálicos con Cerradura](#)” y “[Aislamiento de Equipos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Aseguramiento de Puertas Abiertas de Par en Par en Centros de Computación

Política: Cada vez que sea necesario mantener abiertas de par en par las puertas del centro de computación, la entrada debe estar continuamente monitoreada por un empleado o un guardia del departamento de Seguridad Física.

Comentario: Esta política garantiza que los equipos y la información no serán removidos porque las puertas del centro de computación no estén suficientemente controladas. La política puede también ser utilizada para asegurar que el personal de una agencia de mudanzas no se lleve materiales ajenos, intencional o accidentalmente. Esta política es necesaria porque muchos talleres no hacen cumplir estrictamente los controles de acceso físico, y el centro de computación es probablemente el depósito central de la información importante de la organización. La implementación operacional de la política no tiene que ser difícil. El operador del computador sólo necesita llamar y solicitar al departamento de Seguridad Física el envío de un guardia.

Políticas Relacionadas: “[Pases de Propiedad](#)” y “[Acceso al Centro de Computación](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Equipos en Areas de Información Secreta

Política: Los equipos de impresión, de copiado y de fax no deben estar ubicados en las zonas físicamente aisladas dentro de las oficinas de la Empresa X que contengan información secreta.

Comentario: Esta política evita que las personas copien o impriman la información contenida en el computador, o de otra manera remuevan copias ya impresas de información secreta. Si los equipos para efectuar estos procesos no están dentro del área asegurada, nadie podrá hacer copias no autorizadas de la información allí contenida. Todas las otras vías a través de las cuales la información secreta puede salir también deben estar cerradas. Por ejemplo, una red local aislada puede ser utilizada para evitar que los usuarios envíen la información secreta vía Internet como parte de un

mensaje de correo electrónico. El altísimo enfoque de seguridad que se refleja en esta política funciona mejor si el movimiento de información secreta impresa es estrictamente controlado, quizás con censores que detecten que ha sido removida de un área aislada. Esta política también crea una oficina sin papeles que, cuando es desplegada en áreas de alta seguridad, tiene el potencial de ser más segura que cualquier oficina basada en papeles.

Políticas Relacionadas: “[Estaciones de Trabajo Sin Discos](#)” y “[Operadores de Entrada de Datos](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Altos

5. Señalización de Centros de Computación y Comunicaciones

Política: No debe haber señalización que indique la ubicación de los centros de computación o de comunicaciones.

Comentario: Esta política significa que los avisos con el nombre de la organización, los avisos del centro de comunicación, los avisos en el salón de computación, los avisos del departamento de Sistema Informáticos y los avisos de los grupos de soporte técnico no deben ser visibles desde áreas públicas. La política tiene la intención de prevenir ataques físicos o sabotaje. Además de evitar ataques físicos, la ausencia de avisos ayuda a prevenir ataques a datos, como por ejemplo a través de la colocación de micrófonos ocultos. Un problema con este procedimiento es que los empleados y otros se confundirán y tendrán que pedir direcciones o ser escoltados. Los recepcionistas, los guardias y otros no deben ser tan bien educados como para deshacer la intención de la política. Debe limitarse la cantidad de información sobre direcciones que pueda darse a las personas extrañas sin saber si tienen una razón genuina para estar allí.

Políticas Relacionadas: “[Visitas a las Instalaciones de Computación](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

7.01.04 Trabajo en Areas Seguras

1. Presencia del Personal del Centro de Computación

Política: El centro principal de computación debe tener personal técnico competente asignado todo el tiempo, las 24 horas del día, los siete días de la semana y los 365 días del año.

Comentario: Esta política garantiza mínimo tiempo fuera de servicio y alto nivel de servicio al cliente. La política también garantiza que alguien siempre estará disponible para responder al ataque de un intruso en el momento que ocurra. Para las redes internacionales, como las telefónicas, mantener personal continuamente es una absoluta necesidad. Igualmente esta política se encuentra comúnmente en proveedores de servicios de Internet, organizaciones de Internet y comerciantes de Internet que manejan grandes volúmenes. La política es aplicable en grandes organizaciones que tienen los recursos para mantener una cobertura continua. Organizaciones más pequeñas pueden cambiar la política para referirse al personal que está a una llamada de distancia, en cuyos casos un busca-personas o teléfono celular facilitaría la comunicación. La política también se puede cambiar con el fin de remover la referencia que se hace al sitio principal. Algunas organizaciones tienen a su personal de apoyo en diferentes partes del mundo trabajando, si los otros empleados que se encuentran en husos horarios contiguos también están trabajando. El tener personal disponible continuamente los habilita para notar cosas que los sistemas electrónicos no podrían detectar fácilmente. Por ejemplo, el nivel del río que esta detrás del centro de computación esta subiendo debido a las intensas lluvias, y es inminente una inundación. En algunos casos, tener personal continuo disponible también puede bajar las primas de los seguros. La política es deliberadamente silenciosa cuando se trata de definir "competencia técnica", dejando esta decisión al personal de la gerencia de sistemas informáticos.

Políticas Relacionadas: ["Problemas por Accesos No Autorizados"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Uso de Teléfonos Celulares

Política: No deben utilizarse teléfonos celulares dentro de las salas de computación de la Empresa X.

Comentario: Esta política garantiza que los sistemas de computación y comunicaciones contenidos en un centro de datos están encendidos y funcionando el mayor tiempo posible. Ha habido reportes confirmados acerca de celulares utilizados cerca de servidores de producción, provocando caídas del sistema y corrupción del disco duro. Aparentemente las fuertes señales emitidas por los celulares interfieren con los delicados circuitos de los sistemas de computación y comunicación. Este fenómeno puede no parecer factible, pero las grandes líneas aéreas ahora prohíben que los pasajeros utilicen los celulares durante el despegue y el aterrizaje. Si los celulares pueden afectar los computadores de un avión, también pueden afectar los computadores de un centro de datos. Esta política puede ser ampliada para incluir localizadores de personas de dos vías.

Políticas Relacionadas: ["Teléfonos Celulares o Inalámbricos"](#) y ["Pases de Propiedad"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Trabajo en Areas Restringidas

Política: Los trabajadores nunca deben trabajar solos en áreas restringidas que contengan información sensible.

Comentario: Esta política evita que los trabajadores se aprovechen del hecho de estar solos dentro del área con información sensible. Por ejemplo, un trabajador puede registrar el archivo personal de otro trabajador, algo que no haría si otro trabajador estuviese presente. Dependiendo de las otras políticas que se utilicen en la organización, esta política puede ser ampliada para mencionar información valiosa o crítica. Para hacer la política más restrictiva, la palabra "confidencial" se puede cambiar por "secreta". Esta política garantiza la vigencia de una política de separación de tareas.

Políticas Relacionadas: ["Separación de Tareas"](#) y ["Horario de Areas Restringidas"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

4. Horario de Áreas Restringidas

Política: Los trabajadores autorizados no deben entrar a las instalaciones de la Empresa X donde se maneje información sensible, crítica o valiosa, fuera de las horas de acceso autorizadas.

Comentario: Si los empleados se quedan hasta tarde o si llegan temprano, puede que no estén supervisados y por ello involucrarse en abusos computarizados, como utilizar el computador de otro empleado para ver datos confidenciales. Si los trabajadores se restringen al horario normal, no se involucran en actos de ese tipo porque no van a correr el riesgo de ser descubiertos o que otras personas les impidan realizar esos actos. Esta política es una política de fondo que asegura la efectividad de las políticas de separación de tareas. En la política la palabra "oficiales" puede ser cambiada por "autorizadas" para brindar a la gerencia flexibilidad adicional en el establecimiento del horario de trabajo.

Políticas Relacionadas: "[Separación de Tareas](#)" y "[Trabajo en Áreas Restringidas](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

5. Áreas de Equipos Vacíos

Política: Todas las áreas desocupadas que contengan equipos de sistemas informáticos, deben permanecer cerradas con llave e inspeccionarse periódicamente a través de un sistema de monitor remoto o por un guardia de seguridad.

Comentario: Esta política está motivada parcialmente por los requisitos de las empresas aseguradoras, lo cual es un reflejo de una buena gestión en sistemas informáticos. Cerrar los locales con llave evita que entren espías industriales, ex-empleados disgustados y vecinos curiosos. La inspección de los locales normalmente incluye el confirmar que las puertas están cerradas con llave y que todo parece seguro. Esta política no se aplica sólo a los centros de datos, sino también a oficinas con computadores personales. La adopción e implementación de esta política permite que una organización baje los costos de las primas de los seguros.

Políticas Relacionadas: "[Acceso al Centro de Computación](#)"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

6. Áreas de Equipos de Comunicaciones

Política: Las cassetas telefónicas, las salas de enruteadores y concentradores de red, los espacios para el sistema de correo de voz y áreas similares que contengan equipos de comunicaciones deben mantenerse siempre cerrados con llave, y los visitantes no deben entrar sin la escolta proporcionada por el personal técnico autorizado para monitorear todo el trabajo que se esté efectuando.

Comentario: Esta política evita que terceros puedan colocar micrófonos ocultos en las áreas de comunicaciones de la Empresa X. La política propone evitar que personas no autorizadas dañen o interfieran con equipos críticos necesarios para efectuar las actividades de negocio. Los empleados descontentos encontrarán que es más difícil hacer daño o interferir con estos sistemas altamente complicados si esas áreas están restringidas. Adicionalmente, el uso de una escolta disuade actividades no autorizadas porque cada acción es monitoreada. A pesar de que una escolta puede parecer una pérdida de tiempo del personal técnico, es importante que el personal interno sepa lo que se hizo, por qué se hizo y cómo revertir cualquier cambio efectuado. Mientras se acompaña a un visitante, el escolta puede llenar los papeles de control de los cambios a medida que el visitante hace su trabajo.

Políticas Relacionadas: "[Puertos de Red en Oficinas Vacías](#)" y "[Entregas al Centro de Computación](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

7. Equipos de Grabación de Audio o Video

Política: Las cámaras y los equipos de grabación de audio o de video propios, no deben usarse o estar disponibles dentro de los perímetros controlados de las oficinas de la Empresa X.

Comentario: Esta política tiene la intención de evitar que cualquier equipo de grabación de audio o video se utilice para capturar información confidencial. La información confidencial puede incluir la forma física de un producto nuevo o el plano de distribución de una instalación para procesamiento de datos. La prohibición de tales equipos reduce la posibilidad de usarlos para capturar información confidencial que permanezca en pizarrones, que resulte del intercambio conversacional, o que esté expresada en un memo colocado en el escritorio de un empleado. Algunas organizaciones colocan un aviso al respecto en el escritorio del guardia de entrada. Si se usó una cámara o equipo de grabación

de audio o video, en contravención de esta política, el departamento de Seguridad Física puede confiscar el rollo o la cinta y revelarla, para después regresar el material que no se relaciona con la Empresa X.

7.01.05 Areas Aisladas de Carga y Descarga

1. Entregas al Centro de Computación

Política: Se debe utilizar un área intermedia segura de almacenamiento para guardar los suministros de materiales de computación, equipos y otros materiales entregados.

Comentario: Esta política protege las salas de computación de acceso no autorizado, tal como el del personal de servicio de entregas. Por ejemplo, las puertas de la rampa de carga no deben abrir directamente al salón de computación. Al restringir el movimiento de materiales, esta política también refuerza los controles de acceso a un salón de computación. La política mantiene bajo el riesgo de incendio, al exigir que el papel y otros materiales se almacenen en un sitio distinto al salón de computación. Mantener estos materiales fuera del salón

Políticas Relacionadas: “Prevención del Copiado de Documentos Sensibles” y “Posiciones de las Pantallas de los Computadores”

Política Dirigida a: Todos

Ambientes de Seguridad: Altos

de computación también reduce la exposición de los sistemas a residuos de papel, líquidos de limpieza y otras sustancias potencialmente peligrosas. Esta política también apoya un departamento separado de Recepción que inspeccionará y se responsabilizará por los embarques recibidos y también transportará los bienes a las ubicaciones que los necesitan. Esta política detiene la práctica aquella de guardar los bienes de alto valor en un salón de computación, porque ésta es una de las pocas áreas físicamente seguras.

Políticas Relacionadas: “Mal Funcionamiento del Control de Acceso”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

7.02 Seguridad de los Equipos

7.02.01 Ubicación y Protección de los Equipos

1. Fumar, Comer y Beber

Política: Los trabajadores y visitantes deben abstenerse de fumar, comer o beber en el área de sobrepiso del salón de computación.

Comentario: Aunque parezca un inconveniente para aquellas personas que no quieren salir del salón de computación cuando están trabajando, esta política protege de daños al equipo y a la información. La política también puede ser aplicada a estaciones de trabajo, computadores personales, servidores de redes de área local y otros sistemas no contenidos en el salón de computación. Otro ejemplo serían los sistemas telefónicos privados. Tanto el equipo como el medio de almacenamiento de datos de estos sistemas son susceptibles a daños por las sustancias arriba mencionadas. Químicos volátiles, como pegas y solventes, pueden adicionalmente dañar el medio magnético de almacenamiento y podrían ser mencionados en la política.

También por razones de prevención de incendios, es prudente mantener tales químicos fuera del salón de computación.

Políticas Relacionadas: “Control de Acceso Físico a la Información Sensible” y “Resistencia al Fuego de Centros de Computación”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Ubicación de Sistemas de Computación de Producción

Política: Todos los sistemas computarizados de producción incluyendo, sin limitantes, servidores, cortafuegos, concentradores, enruteadores y sistemas de correo de voz deben estar ubicados físicamente dentro de un centro de datos seguro.

Comentario: Esta política impide que los departamentos y otras unidades organizacionales coloquen equipos de computación de producción en armarios y en otros lugares no protegidos, donde pueden quedar expuestos a sabotaje, cortes de corriente e incendios. Si un sistema de computación funciona como sistema de producción, que se utiliza para las actividades regulares y recurrentes del negocio, debe protegerse colocándolo en una sala de máquinas con dispositivos de seguridad, tales como equipos para control de incendios, generador eléctrico de emergencia, controles de acceso físico y mensajeros remotos de apoyo.

Políticas Relacionadas: “[Aseguramiento de Actividades de Manejo de Información Sensible o Crítica](#)” y “[Ubicaciones de Centros de Computación](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Dirección de los Centros de Computación

Política: La dirección física de todos los centros de computación de la Empresa X es confidencial y no debe ser divulgada a aquéllos que no tengan la necesidad demostrable de conocerla.

Comentario: Esta política asegura que terroristas, saboteadores, espías industriales, hackers y competidores no puedan localizar fácilmente las instalaciones de procesamiento de datos de la Empresa X. Para la correspondencia se recomienda tener un buzón de correo. Los proveedores, consultores y otros terceros que realicen trabajos para la Empresa X, necesitan conocer la dirección sólo si necesitan ir al sitio. Las guías telefónicas de la compañía tampoco deben mostrar la dirección de estas instalaciones. No debe existir ningún tipo de aviso a nivel de calle indicando la ubicación del centro de procesamiento de datos de la Empresa X. Esta política puede ser ampliada para incluir los centros de control de redes, archivos de registros y otras instalaciones que manejen o almacenen información. A pesar de que se hace referencia a un centro de computación que normalmente incluye un mainframe y sistemas más amplios, esta política es igualmente aplicable a sistemas más pequeños como lo son los computadores personales, las estaciones de trabajo y los sistemas cliente-servidor.

Políticas Relacionadas: “[Naturaleza y Ubicación de la Información de la Organización](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Controles Ambientales del Centro de Computación

Política: La gerencia local debe suministrar y mantener adecuadamente los sistemas de prevención y supresión de incendios, aire acondicionado, control de humedad y otros sistemas de protección de ambientes computarizados, en todos los centros de computación de la Empresa X.

Comentario: Estos sistemas de apoyo ambiental son esenciales para el funcionamiento continuo de los computadores y las comunicaciones. Esta política requiere que la gerencia local suministre los sistemas necesarios para los computadores que manejan aplicaciones críticas de producción. Esta política puede ser empleada por los usuarios finales para obligar a los gerentes locales y departamentales a cumplir los requerimientos definidos por un grupo gerencial centralizado de tecnología informática. Por ejemplo, los usuarios de computadores personales que manejen una aplicación crítica pueden necesitar, pero no tener, un sistema de electricidad sin interrupción (UPS) y estos usuarios estarán presionando a la gerencia local para que adquiera dicho equipo. La política podría ser utilizada entonces para obligar a la gerencia a conseguir el sistema UPS. La distribución o descentralización de los sistemas informáticos ha traído como consecuencia que ahora es la gerencia local quien toma las decisiones que anteriormente tomaba el departamento de Tecnología Informática. Para garantizar que la gerencia local tome las decisiones correctas, se requiere una política como ésta. Los sistemas de computación más pequeños pero más avanzados no tienen los mismos requerimientos de ambiente que los más grandes y viejos, como por ejemplo la necesidad de aire acondicionado. Esta política es deliberadamente ambigua acerca de los sistemas que se deben utilizar para controlar el ambiente, porque estos son determinados por factores como la ubicación geográfica, sistemas tecnológicos empleados y las necesidades del negocio. La política asume que la palabra "crítica" se definió en otra política.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Equipo de Protección Eléctrica](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Protección Contra Electricidad Estática

Política: Si las condiciones del tiempo y del edificio presentan riesgo de descarga de electricidad estática, todos los computadores personales y estaciones de trabajo deben ser provistos de equipos con protección antiestática aprobados por el departamento de Sistemas Informáticos.

Comentario: Esta política garantiza que los equipos de computación estarán correctamente configurados para prevenir la pérdida de datos, daño a los sistemas y el tiempo fuera de servicio. Muchas veces en climas fríos, donde existen sistemas de calefacción, la electricidad estática es un problema importante. Específicamente, el circuito integrado de los microprocesadores pueden quemarse y puede borrarse la información que mantienen en memoria. Medidas específicas de control como alfombras y barras contra la electricidad estática y equipo aprobado de conexión a tierra deben ser mencionados en esta política. Las medidas específicas de control no están incluidas en esta política porque están sujetas a cambios frecuentes a través del tiempo. Esta política se puede ampliar con el fin de incluir sistemas de comunicación y de computación. Si la organización utiliza una tecnología más tradicional, puede añadir la palabra "terminales" a la política justo al lado de la referencia "estaciones de trabajo".

Políticas Relacionadas: ["Equipo de Protección Eléctrica"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Dispersión de Sistemas Computacionales

Política: Los sistemas de computación y de comunicaciones deben estar geográficamente dispersos siempre que sea posible, si esto no perturba indebidamente el funcionamiento operacional, ni pone en peligro la seguridad ni aumenta los costos.

Comentario: Esta política enfatiza los beneficios relativos a la planificación de contingencias de la computación distribuida. La mención de las maneras de perjudicar la seguridad en una política puede parecer contraproducente, porque puede sugerir ideas a las personas, pero esta política se mantiene en un nivel general y no da instrucciones específicas de cómo causar daños específicos a la Empresa X. Por el contrario, expresa una intención de diseño que es totalmente consistente con la evolución de los sistemas, particularmente con los sistemas cliente-servidor. Muchos de los sistemas más pequeños, como el sistema

cliente-servidor, a menudo tienen medidas poco adecuadas de seguridad, así que se necesita conseguir un equilibrio. En otras palabras, la seguridad ampliada por la planificación de contingencias que se logra con la descentralización se intercambia en parte por la reducción de la seguridad en el control de acceso.

Políticas Relacionadas: ["Protección de la Información"](#) y ["Requerimientos para el Soporte de Emergencias y Desastres"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Infraestructura de Respaldo para Centro de Datos

Política: La Empresa X debe dividir sus centros de procesamiento de datos en tres instalaciones distintas y físicamente aisladas, cada una capaz de manejar todos los servicios de los sistemas críticos de información de producción, y no deben compartir la misma subestación eléctrica de la compañía local, ni la misma central de la compañía telefónica.

Comentario: Esta política de ubicación de los centros de datos está siendo adoptada por las grandes organizaciones como una alternativa estratégica al uso de servicios de respaldo comercial de terceros. La política permite a la organización que la adopte, reasignar dinámicamente las actividades críticas de procesamiento de producción a otro centro de datos en caso de que uno de sus centros no esté disponible. La política está dirigida a personal de los sistemas informáticos, para que puedan reorganizar internamente los sistemas informáticos con el fin de suministrar un mayor grado de resistencia contra amenazas de desastres y ataques terroristas. La política puede ser ampliada para incluir elementos separados y aislados de infraestructura tales como sistemas de transporte diferentes y gobiernos locales diferentes. Para una disponibilidad mayor del sistema, las palabras "subestación de la compañía eléctrica" pueden ser cambiadas por "red de la compañía eléctrica" y las palabras "central de la compañía telefónica" por "compañía telefónica". La palabra "tres" en la política podría ser cambiada a "dos", pero ello significaría perder cierta flexibilidad en la reubicación del procesamiento de producción.

Políticas Relacionadas: ["Múltiples Operadoras Telefónicas"](#) y ["Punto Central de Falla de la Red"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

8. Sistemas de Computación Pertenecientes a Trabajadores

Política: Los trabajadores no deben traer a las instalaciones de la Empresa X sus propios computadores, periféricos o software, sin la debida autorización de sus jefes de departamento.

Comentario: Esta política evita la propagación de virus, discusiones sobre la propiedad de hardware y software y la remoción no autorizada de hardware y software o datos cuando un trabajador termina su relación de trabajo con la empresa. La política es deseable porque garantiza que todos utilizarán el mismo tipo de software. Esta política es particularmente importante para los computadores personales (PC), estaciones de trabajo y sistemas cliente-servidor, para los que la propiedad no siempre está clara. Esta política puede estar apoyada por otra política que requiera que todos los computadores y equipos de comunicación deben tener un pase de propiedad antes de poder ser removidos de las instalaciones de la Empresa X.

Políticas Relacionadas: “[Pases de Propiedad](#)” y “[Procura de Hardware y Software](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

9. Llaves de las Estaciones de Trabajo

Política: Todas las estaciones de trabajo de escritorio de la Empresa X deben utilizar cierre con llave metálica para controlar el acceso de personas no autorizadas, reteniendo el gerente del departamento una copia de la llave.

Comentario: Esta política, aunque algo vieja, puede ser utilizada en conjunción con los controles de acceso basados en contraseñas, tal como el mecanismo de protección de inicialización de computadores que emplea contraseñas fijas. Esta política evita que personas no autorizadas tengan acceso a las estaciones de trabajo, que podrían contener información sensible almacenada. El problema con este procedimiento es que los usuarios perderán u olvidarán sus llaves de metal, en cuyo caso no podrán utilizar sus estaciones de trabajo. Es por esto que una llave de respaldo es entregada al gerente del departamento. La palabra "escritorio" fue usada en la política para eximir los computadores portátiles como los laptops. Para implantar esta política y debido a que usualmente no traen llave, algunos

computadores necesitarán la instalación de algunos aditamentos de seguridad que utilicen llaves para cubrir el teclado, la apertura del disco flexible u otro componente. Dependiendo de la configuración del mecanismo de cierre, algunas llaves también se pueden utilizar para evitar que personas no autorizadas abran el cajón del computador, para robarse componentes como el módem o las memorias.

Políticas Relacionadas: “[Gabinetes de Archivo con Llave](#)” y “[Protección de la Reinicialización Basada en Contraseña](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Puertas de Gabinetes de Equipos

Política: Todas las puertas de los estantes y gabinetes de equipos de computación y comunicaciones ubicados en el centro de computación deben permanecer cerradas con llave, a menos que un técnico autorizado esté efectuando reparaciones, mantenimiento o alguna actividad de reconfiguración.

Comentario: Esta política establece otra capa más al control del acceso físico al equipo de computación ubicado en un centro de datos seguro. En muchas organizaciones un gran número de personas pueden entrar al centro de datos, incluyendo programadores, operadores y analistas de desempeño. Aunque es deseable mantener el número de personas a un mínimo para así reducir las oportunidades de sabotaje y otros tipos de abusos, a veces no es práctico o políticamente oportuno. Como alternativa, hay que considerar poner paredes adicionales o jaulas de metal para separar secciones del salón en diferentes zonas, donde cada una posea su propio nivel de seguridad. También se debe considerar cerrar con llave los gabinetes en donde se encuentran los equipos de producción. Esta política prefiere la opción anterior. Se puede redactar una política sobre el cierre de rejillas de metal o la colocación de paredes normales dentro del centro de datos en el mismo formato en que se encuentra esta política.

Políticas Relacionadas: “[Gabinetes de Archivo con Llave](#)” y “[Requisitos de Seguridad para Teletrabajo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

11. Sistemas Comerciales y Financieros en Internet

Política: Todos los servidores y equipos de comercio de Internet, así como los sistemas que procesen o faciliten el proceso de transferencias y otras actividades financieras, deben estar físicamente aislados y asegurados.

Comentario: Esta política segregá y protege de manera separada los computadores que manejan dinero digitalizado, como parte del esfuerzo realizado para reducir la posibilidad de estafas. Si los operadores de computación son capaces de reiniciar un servidor, también podrán cambiar los controles de acceso, cambiar los parámetros del sistema operativo, o de alguna manera comprometer la seguridad del sistema. El permitir acceso físico a estos sistemas también puede permitir que personas no autorizadas roben cintas de respaldo que puedan contener números de tarjetas de crédito, números de cuentas bancarias, u otra información que pueda ser utilizada para cometer delitos. Esta política reconoce que algún nivel de seguridad física es necesario antes de obtener una verdadera seguridad informática. Esta política asume que un centro de computación está cerrado con llave y que sólo se permite la entrada a un número restringido de personas. Esta política suministra un nivel de control de acceso físico adicional más allá de las puertas del centro de computación. Esta política es totalmente consistente con las especificaciones de diseño de un centro de computación normal de servicios de hospedaje para sitios de Internet, que típicamente utiliza jaulas de metal cerradas con llave para separar las máquinas de varios suscriptores. Pero aunque una organización realice su propio hospedaje, el comercio de Internet y los servidores financieros relacionados se deben ubicar en salones seguros y separados, o se deben mantener de alguna otra manera aislados físicamente del resto de las máquinas del centro de computación.

Políticas Relacionadas: “Aislamiento de Equipos” y “Aseguramiento de Actividades de Manejo de Información Sensible o Crítica”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

12. Aislamiento de Equipos

Política: Los equipos de computación y comunicaciones manejados por personal de la Empresa X, deben estar físicamente aislados de los equipos manejados por terceros.

Comentario: Esta política impide que terceros tengan acceso innecesario a los equipos de computación y comunicación de la Empresa X. El acceso físico puede permitir que personas no autorizadas reinicien el sistema operativo, lo que les permitiría asumir el control del sistema de control de acceso, robar medios magnéticos como cintas de respaldo y sabotear equipos. Si el equipo está mezclado en el centro de datos, entonces los terceros deben estar en el mismo salón donde está ubicado el equipo que maneja la Empresa X. Pero si se utilizan salones separados, se pueden usar los controles de acceso físico. No es necesario el uso de salones separados. Se puede utilizar una jaula de metal cerrada, o se pueden añadir particiones de vidrio a un salón existente. Esta política es relevante, por ejemplo, cuando la Empresa X tiene equipo contenido en un centro de datos de una organización de servicios de hospedaje para comercio en Internet. Los controles de acceso físico para el equipo que maneja la Empresa X pueden ser un requisito previo al uso de herramientas de administración de redes remotas y para establecer operaciones nocturnas.

Políticas Relacionadas: “Acceso a Sistemas de Computación y Comunicación,” “Distintas Zonas de Riesgo de Incendio,” y “Aseguramiento de los Sistemas de Computación o Comunicación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

13. Ubicaciones de Centros de Computación

Política: Todos los centros nuevos de computación o de comunicación de la Empresa X, deben estar ubicados en un área donde exista baja probabilidad de desastres naturales, accidentes serios causados por el hombre, motines y otros problemas relacionados.

Comentario: Esta política requiere que la gerencia considere con anticipación las consecuencias de ubicar un centro de computación o de comunicación en un área peligrosa. Comúnmente se toma la decisión de ubicar una instalación y sólo después es que se notan los riesgos serios. Esta política requiere que la gerencia prepare una declaración de impacto sobre la seguridad. La frase “Centros de computación o de comunicación” puede ser clarificada, aunque es deliberadamente ambigua para dar a la política una aplicación general que pueda ser extendida a sistemas departamentales, servidores de redes de área local, sistemas cliente-servidor y otros sistemas más pequeños.

Políticas Relacionadas: “Proveedores Redundantes de Suministros Básicos” y “Ubicación del Centro de Computación y Comunicaciones”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

14. Construcción del Centro de Computación

Política: Los centros de computación y comunicación de la Empresa X, tanto nuevos como remodelados, se deben construir de manera tal que estén protegidos contra incendios, daños causados por agua, vandalismo y otras amenazas conocidas o que puedan ocurrir en las instalaciones correspondientes.

Comentario: Esta política requiere que los encargados de la construcción o remodelación de los centros de computación o comunicación consideren los riesgos de seguridad locales antes de la construcción. La política es una versión específica orientada a la construcción con las normas de debido cuidado.

Políticas Relacionadas: “Normas de Implantación de Controles” y “Ubicaciones de Centros de Computación”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

15. Precauciones ante Daños por Agua

Política: Todos los locales de la Empresa X que albergan equipos de computación y comunicación deben cumplir los requerimientos mínimos de prevención contra daños por agua y las precauciones mínimas de alarma establecidas por el departamento de Seguridad Informática, ubicándolos por encima de la planta baja y del nivel de inundaciones de desagües y ríos cercanos, con un sistema de drenaje adecuado y no ubicados debajo de tanques de agua o tuberías de agua.

Comentario: Esta política establece unas normas mínimas de protección contra los daños causados por agua a equipos de computación y comunicación. Debido a que son equipos eléctricos, existe el peligro de electrocución en adición a los daños severos que causa al equipo si se moja cuando está funcionando. Aunque la electricidad esté apagada, muchos tipos de equipos están tan finamente calibrados que cualquier cantidad de sucio, polvo u oxido que entre en el equipo con el agua puede causar un mal funcionamiento, aun cuando el equipo se seque completamente. Estas son algunas de las razones de porqué muchas instalaciones utilizan extintores de fuego químicos en vez de rociadores de agua. La política no hace mención de rociadores de agua, permitiendo así que el departamento de Seguridad Informática tome las decisiones que considere convenientes.

Políticas Relacionadas: “Presencia del Personal del Centro de Computación” y “Alarms del Centro de Computación”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

16. Alarmas del Centro de Computación

Política: Todos los centros de computación de la Empresa X deben estar equipados con sistemas de alarma contra incendios, agua e intrusión física que automáticamente alerten a aquéllos en capacidad de tomar medidas inmediatas.

Comentario: Esta política garantiza la inclusión de sistemas adecuados de alarma en todos los centros de computación. El alcance se puede cambiar para incluir los centros de operación de redes. Debido a la reducción de los precios de los computadores, el hardware de producción se queda guardado en armarios o en oficinas normales que no están debidamente protegidas con alarmas. A medida que la tecnología mejora, los sistemas protectores de las grandes máquinas ya no se

utilizan en las máquinas más pequeñas. Con respecto a quienes están en capacidad de tomar medidas inmediatas, los bomberos pueden ser llamados por una alarma de incendio, mientras que un guardia puede ser llamado si se detecta agua y la policía si entra alguien no autorizado. Las especificaciones de estas alarmas deliberadamente se han dejado fuera de esta política. La política sólo dice que deben ser instaladas. Si la política parece algo costosa, puede ser restringida sólo para centros de computación que contengan equipos de soporte para actividades críticas del negocio, tales como el comercio en Internet. Alarmas de incendio, inundaciones y entradas de intrusos pueden conectarse a un sistema de administración de la red.

Políticas Relacionadas:“[Pases de Propiedad](#)” y “[Sistemas de Detección de Intrusos](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

7.02.02 Suministro Eléctrico

1. Equipo de Protección Eléctrica

Política: Todos los computadores personales y estaciones de trabajo deben estar equipados con sistemas que suplan corriente eléctrica sin interrupciones, filtros de potencia eléctrica o supresores de alzas de voltaje aprobados por el departamento de Sistemas Informáticos.

Comentario: Un alto porcentaje de los problemas de los computadores son atribuibles a variaciones en el suministro eléctrico, como las alzas de voltaje, impulsos, bajas de voltaje y apagones. Esta política es importante igualmente para minicomputadores, super-minicomputadores y otros sistemas. En la mayoría de los casos, sin embargo, los sistemas multiusuario ya traen suficientes medidas de protección eléctrica. La intención de esta política es requerir que los sistemas que dependen de la gerencia local o departamental sean equipados con los equipos apropiados de acondicionamiento eléctrico. El tipo específico de protección de corriente que se necesita es una función de la criticidad del sistema, y no se especifica en la política.

Políticas Relacionadas:“[Protección Contra Electricidad Estática](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

2. Proveedores Redundantes de Suministros Básicos

Política: Todos los nuevos centros de computación y de comunicaciones de la Empresa X deben estar ubicados de tal forma que tengan acceso a dos compañías suplidoras de energía eléctrica y dos compañías de teléfonos.

Comentario: Esta política tiene la intención de establecer un objetivo mínimo de diseño para los individuos que están diseñando los nuevos centros de computación y comunicación. La política especifica que debe haber más de un suplidor de servicios de electricidad. El agua se puede incluir en esta política, pero rara vez se necesita para apoyar los sistemas de computación y comunicación, excepto para equipos heredados como los equipos mainframe que la utilizan para el enfriamiento. El agua se almacena mucho más fácilmente y es menos costosa que la electricidad. En la política puede incorporarse una previsión adicional que establezca que las líneas eléctricas y los teléfonos deben correr en postes separados o a través de conductos separados. Sin este requerimiento de tendidos separados, una grúa o una excavadora podría cortar ambas líneas de suministro.

Políticas Relacionadas:“[Ubicaciones de Centros de Computación](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

7.02.03 Seguridad en el Tendido de Cables

1. Cables Eléctricos y de Telecomunicaciones

Política: La instalación y el mantenimiento de los cables de electricidad y de telecomunicaciones deben ser efectuados por un diseñador certificado de distribución de comunicaciones, que cumpla las normas establecidas de seguridad de la industria.

Comentario:Esta política garantiza que todos los cables de los sistemas de computación se instalarán y mantendrán correctamente, para evitar cualquier intercepción no autorizada de la transmisión de datos o daños al sistema. Los datos pueden ser fácilmente interceptados durante una transmisión si no está protegido el acceso a

las líneas de telecomunicaciones. Hay muchas normas que rigen la correcta instalación de estas líneas que llevan a cabo profesionales entrenados, quienes garantizan que las telecomunicaciones no se verán comprometidas. Igualmente, se deben proteger los cables de electricidad para evitar daños o interrupciones de servicio a los sistemas de computación.

Políticas Relacionadas:“[Cambios en la Línea de Comunicación](#)” y “[Registro de Línea de Modem](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

7.02.04 Mantenimiento de Equipos

1. Productos de Sistemas Informáticos

Política: Todos los productos de hardware y software se deben registrar con su proveedor correspondiente inmediatamente después de que el personal de la Empresa X reciba los productos nuevos o actualizados del sistema informático, o tan pronto se determine que los productos no se han registrado todavía.

Comentario:Esta política garantiza que todo el hardware y software está registrado con los proveedores. Esto indirectamente garantiza que todos estos productos han sido debidamente pagados, reduciendo así las copias de software y robos de equipos. El registro adecuado significa que el usuario va a recibir notificaciones de errores, actualizaciones y otras ofertas de relevancia. El registro también permitirá que la organización usuaria obtenga apoyo técnico, telefónico y de cualquier otro tipo. El registro significa que el proveedor servirá de ayuda en el caso de un desastre o una emergencia. Bajo estas circunstancias se pueden obtener copias de reemplazo gratuitas o al menos a un costo mínimo, si el producto fue registrado previamente. Esta política también puede servir de ayuda en un juzgado o durante una auditoría de software, porque demuestra que la gerencia intenta genuinamente garantizar que todas las copias en uso de dicho software son copias autorizadas.

Políticas Relacionadas:“[Duplicación de Software](#)” y “[Copias de Software](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

2. Mantenimiento Preventivo

Política: Debe ejecutarse regularmente el mantenimiento preventivo de todos los sistemas de computación y comunicación.

Comentario:La política es deliberadamente amplia en la definición de mantenimiento preventivo. La gerencia media debe determinar cuál mantenimiento preventivo es el adecuado. El mantenimiento preventivo puede incluir el reemplazo de viejas cintas magnéticas por nuevas, limpieza y lubricación de la unidad del disco y limpieza debajo de los pisos falsos. Las estadísticas demuestran que el mantenimiento preventivo puede reducir el tiempo de parada de los sistemas de computación. Esta política es totalmente consistente con los sistemas de mantenimiento contratados que periódicamente notifican al proveedor sobre el estatus interno del sistema, requiriendo automáticamente ciertas acciones correctivas, tal como el reemplazo de una tarjeta de circuito en la cual se han detectado muchas fallas. Si el alcance de esta política parece ser muy amplio, la política puede ser restringida a "sistemas de produc-

ción". El mantenimiento preventivo es importante para los computadores personales, redes de área local, sistemas cliente-servidor, sistemas de comercios en Internet y otros sistemas pequeños, al igual que para los equipos mainframe y sistemas grandes. Las palabras "sistemas de computación y comunicación" pueden referirse tanto al software y la información recopilada como al hardware.

Políticas Relacionadas: "Niveles de Soporte de Interrupción del Negocio" y "Mantenimiento de Equipos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Mantenimiento de Equipos

Política: Todos los equipos de los sistemas informáticos utilizados en el proceso de producción, deben conservarse de acuerdo a las especificaciones e intervalos de servicio recomendadas por el proveedor, con reparaciones y servicios ejecutados solamente por personal de mantenimiento calificado y autorizado.

Comentario: Esta política garantiza que los equipos de los sistemas informáticos continuarán operando como deben, apoyando a la organización en el cumplimiento de su misión. El tiempo fuera de servicio puede ser un problema serio, porque paraliza las actividades del sistema informático. Esta política no menciona el tamaño del sistema y se aplica a computadores personales y sistemas mayores mencionados anteriormente. Esta política puede ser utilizada para informar a los usuarios que no deben tratar de reparar sus propios equipos de computación, sino llamar al Centro de Atención al Usuario o cualquier otro personal autorizado del departamento de Sistemas Informáticos.

Políticas Relacionadas: "Mantenimiento Preventivo"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Retención de Hardware y Software

Política: El hardware y software requeridos para leer los medios de almacenamiento de datos en los archivos de la Empresa X deben estar a la mano, correctamente configurados y mantenidos en condiciones operativas.

Comentario: Esta política requiere que el hardware y software anticuados se mantengan de tal forma que se pueda acceder a los datos archivados. Por ejemplo,

muchas organizaciones tienen rollos de cinta de nueve canales y otros medios viejos de almacenamiento, los cuales ya no se utilizan en producción. Pueden haber eliminado el hardware para leer cintas de nueve canales, pero mantienen las cintas con propósitos legales, históricos y otros. Esta política prohíbe eliminar dichos equipos por las demoras que se generarán si la información en esas cintas de nueve canales necesita ser recuperada. Nada de lo mencionado en esta política evita que una organización mueva los datos contenidos en estos formatos a un medio de almacenamiento actualizado, lo cual es recomendable para asegurar que todos los datos sean recuperables y para disminuir a un mínimo la cantidad de dispositivos de hardware disponibles.

Políticas Relacionadas: "Pruebas de Medios de Almacenamiento de Archivos" y "Versiones de Software para Firmas Digitales y Cifrado de Archivos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Modificaciones a Computadores

Política: Los equipos de computación suministrados por la Empresa X no deben alterarse de ninguna manera ni añadirseles nada, sin el conocimiento y autorización de la gerencia del departamento.

Comentario: Esta política garantiza que los usuarios sabrán que no deben alterar los equipos suministrados por la Empresa X. Tales alteraciones pueden derrotar una de las varias medidas de seguridad. Por ejemplo, un sistema protector de reinicialización, que requiere una clave cuando el sistema es encendido, puede impedir a un usuario entrar al computador. Las alteraciones también pueden ser usadas deliberadamente para evitar las medidas de seguridad. La política prohíbe de manera indirecta el robo de componentes internos, como los chips de memoria. La política garantiza que el equipo asignado a un usuario es el equipo que será devuelto cuando el usuario abandone la Empresa X. Esta política no es necesaria si los usuarios sólo usan sus computadores en la oficina. Cuando los computadores son trasladados fuera de las instalaciones de la empresa, la necesidad de tener esta política aumenta dramáticamente. Aunque es de menos importancia, los equipos independientes de comunicación, como el módem externo, también pueden incluirse dentro del alcance de esta política.

Políticas Relacionadas: "Equipo de Teletrabajo" y "Computadores Portátiles con Información Sensible"

Política Dirigida a: Usuarios finales**7.02.05 Seguridad de Equipos Fuera de las Oficinas****1. Autorización de Uso de Equipo Fuera de Sede**

Política: La gerencia debe autorizar el uso de equipos de la Empresa X fuera del área de la empresa.

Comentario: La política tiene la intención de garantizar que la gerencia tendrá conocimiento y autorizará la salida de cualquier equipo a ser trasladado fuera de las instalaciones de la Empresa X. La gerencia debe determinar la necesidad de que el equipo sea trasladado y garantizar que se sigan las medidas apropiadas de seguridad mientras el equipo está fuera del área. Estas incluyen muchos de los mismos controles que se aplican

Ambientes de Seguridad:Todos

cuando el equipo está dentro de las instalaciones de la Empresa X. Por ejemplo, el equipo nunca debe ser dejado sin atención y debe estar vigente un seguro adecuado. Cuando se tenga dudas, la gerencia debe aplicar los mismos controles de seguridad que se aplican para los equipos locales.

Políticas Relacionadas:“[Remoción de Información Sensible](#)” y “[Requisitos de Seguridad para Teletrabajo](#)”

Política Dirigida a:Todos**Ambientes de Seguridad:**Todos**7.02.06 Disposición Segura o Re-Utilización de Equipos****1. Liberación de Componentes Usados**

Política: Seguridad Informática debe certificar que toda la información sensible ha sido removida de cualquier componente del sistema informático utilizado para los negocios de la Empresa X, antes de entregar los componentes a terceros.

Comentario: Esta política evita la entrega de información sensible a terceros. En la creencia de que se trata de reciclaje de equipos obsoletos, muchos gerentes locales donan o venden computadores personales viejos a instituciones de caridad, colegios o proveedores de equipos usados. Estos gerentes pueden no haber tomado las precauciones necesarias para remover toda la información sensible de los discos duros, la ubicación de memorias no volátiles y otros medios de almacenamiento. Esta política transfiere la responsabilidad de la remoción de los datos desde la gerencia local hasta el departamento de Seguridad Informática y garantiza que ningún equipo o medio de almacenamiento donado o vendido contiene información. Esta transferencia de responsabilidades es apropiada porque los gerentes locales a menudo no poseen la pericia suficiente como para determinar si toda la información sensible ha sido removida. La transferencia es también recomendable porque le permite al departamento de Seguridad Informática hacer una evaluación de riesgo específico con el fin de determinar si el equipo o medio puede ser adecuadamente desensibilizado, o si es necesario destruirlo. Esta política también evita publicidad

embarazosa proveniente de escapes de información y garantiza que el departamento de Seguridad Informática estará al tanto de cuáles terceros están recibiendo medios y equipos. Algunos querrán excluir de esta política ciertos equipos, tales como teléfonos, fax o copiadoras, que no tienen capacidad de almacenamiento. Esta política complementa aquellas políticas que establecen que la compra de equipos de sistemas informáticos debe estar centralizada.

Políticas Relacionadas:“[Procura de Hardware y Software](#)” y “[Transferencia de Información Sensible](#)”

Política Dirigida a:Gerencia y personal técnico**Ambientes de Seguridad:**Medianos y altos**2. Disposición de Información y Equipos**

Política: Los gerentes departamentales son responsables de la disposición de la propiedad sobrante que ya no se necesita para las actividades del negocio, en concordancia con los procedimientos establecidos por el departamento de Seguridad de Informática, incluyendo la remoción irreversible de información y software.

Comentario: El borrar un archivo generalmente no es suficiente. Los archivos deben ser purgados o repetidamente re-escritos por utilidades de sistemas distintas para que realmente sean irrecuperables. Este proceso puede ser complejo, así que el departamento de Seguridad de Informática usualmente emite distintos

procedimientos. Por la forma en que está redactada esta política, pueden cambiarse los procedimientos a medida que cambie la tecnología sin necesidad de modificar la política. Mientras el enfoque de esta política frecuentemente es al equipo, la preocupación real es la información almacenada en el equipo. Esta política también evita violaciones casuales de los términos de la licencia del software registrado.

7.03 Controles Generales

7.03.01 Política sobre Pantallas y Escritorios Limpios

1. Escritorios Limpios — Horas No Hábiles

Política: Fuera del horario normal de trabajo, todos los trabajadores deben despejar sus escritorios y áreas de trabajo, de tal manera que todos los datos valiosos o sensibles estén resguardados adecuadamente.

Comentario: Esta política es una versión modificada de la política de escritorios limpios. La política tradicional requiere que toda la información sea resguardada, a menos que esté equivocada la apreciación de la persona sobre la relativa confidencialidad de la información. La política revisada aquí presentada está diseñada para usuarios de computadores personales y estaciones de trabajo que frecuentemente dejan discos flexibles y hojas impresas sobre sus escritorios. Esta política evita que personas que estén en el edificio fuera del horario de trabajo, tengan acceso a información confidencial. Las formas para resguardar adecuadamente la información pueden estar especificadas en otra política o en un anexo con la explicación. Esta política tiene un efecto secundario positivo y es que los escritorios y áreas de trabajo, se mantendrán en perfecto orden. Otro efecto positivo es que los materiales dejados afuera son más propensos a daño o destrucción en un incendio, explosión u otro desastre. En algunos casos la palabra "sensible" puede ser reemplazada por menciones específicas de clasificaciones de datos sensibles de la organización. La política puede ser ampliada para incluir la mención de receptores de correo interno, máquinas de fax desatendidas, pizarrones en salones de conferencia y otros lugares donde la información sensible pudiera estar al descubierto. A pesar de ser obvio para algunos, algunas organizaciones específicamente incluyen en una política de escritorio limpio la mención de que la política no está dirigida a desanimar a los trabajadores a trabajar fuera de horario.

Políticas Relacionadas: "[Transferencia de Información Sensible](#)" y "[Procedimientos para la Destrucción de la Información Sensible](#)"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

Políticas Relacionadas: "[Clasificación de Datos en Cuatro Categorías](#)" y "[Escritorios Limpios — Uso Activo](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Escritorios Limpios — Uso Activo

Política: A menos que la información esté siendo utilizada por personal autorizado, los escritorios deben mantenerse limpios y libres fuera del horario normal de trabajo, con toda la información bajo llave.

Comentario: Esta política de escritorios limpios intenta evitar la divulgación no intencional de información sensible. La política refleja la actitud de la gerencia en el sentido de no confiar en que los trabajadores sabrán lo que se debe o no guardar bajo llave. La política asume que los trabajadores llegan y hacen su trabajo en el horario normal de trabajo, por ejemplo, desde las 9:00 AM hasta las 5:00 PM. Muchas organizaciones se han acogido a los horarios flexibles, y por lo tanto esta política debe ser modificada para dar una mejor descripción del término fuera de horario. Un efecto secundario positivo de esta política es que requiere un ambiente limpio y ordenado, lo cual es apreciado donde se valora la apariencia física. La política supone que la organización dispone del espacio físico y los recursos financieros para suministrar a su personal archivadores con llave en las cerraduras, cajas fuertes y otros contenedores seguros.

Políticas Relacionadas: "[Escritorios Limpios — Horas No Hábiles](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

3. Manejo de Información en Otros Turnos

Política: La información sensible debe estar siempre bajo llave en contenedores cerrados autorizados para información sensible, y no debe ser desatendida en ninguna ubicación insegura durante el segundo o tercer turno.

Comentario: Esta política garantiza que la información sensible no será abandonada en una ubicación donde alguna persona no autorizada pueda verla o robarla sin ser descubierta. Es muy factible que ocurra en el segundo o tercer turno, porque es durante estos turnos que hay pocas personas para darse cuenta de que algo anda mal. Esta política hace una nueva distinción entre las horas cuando hay muchas personas en el sitio y esas horas donde hay menor cantidad de personas. La política supone que la organización que la adopta no tiene horas no hábiles, sino sólo algunos turnos donde hay menos personas trabajando. La política supone que la palabra "sensible" está definida en otra parte.

Políticas Relacionadas: ["Escritorios Limpios — Horas No Hábiles"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

4. Areas Desatendidas

Política: Cuando no esté en uso, la información sensible que se deje en un salón no vigilado, debe mantenerse bajo llave en contenedores apropiados.

Comentario: Esta política define cuándo es aceptable dejar información sensible en un escritorio. La política claramente dice que esto sólo puede suceder si el salón no está vigilado. Otra posible excepción también puede permitirse si la información se deja en un área donde todas las personas están autorizadas para ver la información confidencial. Esta excepción adicional puede ser añadida a la política. La política también puede ser ampliada para indicar que la última persona en salir del área que contenga información sensible debe asegurarse que toda esa información esté debidamente resguardada. Esta política asume que la palabra "sensible" ha sido definida en otros materiales relacionados con las políticas.

Políticas Relacionadas: ["Clasificación de Datos en Cuatro Categorías"](#) y ["Cubrir Información Sensible"](#)

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Almacenamiento de Información Sensible

Política: Todas las copias impresas y todos los medios de computación que contengan información sensible que no esté siendo utilizada por trabajadores autorizados, o cuando no sea claramente visible en un área donde están trabajando personas autorizadas, deben guardarse bajo llave en archivadores, escritorios, caja fuerte u otro tipo de mobiliario.

Comentario: Esta política tiene la intención de suministrar orientación específica a los usuarios finales y otros sobre el manejo adecuado del almacenamiento de la información sensible. Se aplica particularmente a los usuarios de computadores personales y estaciones de trabajo, que con frecuencia dejan un disquete y copias impresos sobre su escritorio. Se pueden realizar auditorías periódicas durante la noche a los escritorios para hacer cumplir esta política. En el título, la palabra "sensible" puede ser remplazada con la mención específica de las clasificaciones de datos sensibles que tenga la organización.

Políticas Relacionadas: ["Clasificación de Datos en Cuatro Categorías"](#) e ["Información Sensible en Computadores Personales"](#)

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Apagado de Computadores

Política: Con excepción de los computadores independientes colocados en áreas con controles estrictos de acceso físico, deben apagarse al final del día, a la hora de almuerzo, y al terminar una sesión, todos los computadores que hayan estado usándose para procesar información secreta.

Comentario: Esta política tiene la intención de concientizar a los usuarios en el sentido de que la información confidencial puede ser escarbada de la memoria de un computador. Dado que la mayoría de los computadores tienen memorias volátiles, esta información se borrará al apagarse la máquina. En algunos casos, dependiendo del tipo de chip utilizado, la memoria no es volátil. En estos casos la información no será borrada, y otras acciones serán necesarias para remover la información residual. En reconocimiento a la existencia de memorias no volátiles, la política pudiera decir, "ver la documentación del fabricante". Un computador apagado es mucho más difícil de manipular remotamente. Si el equipo está apagado, será más difícil realizar una entrada forzosa. La política es particularmente relevante para servidores departamentales independientes,

computadores personales y estaciones de trabajo ubicadas en un ambiente de oficina abierto. La política supone que otras políticas instruyen al usuario en el sentido de no almacenar información en sistemas que tengan controles de acceso inadecuados. Esta política adicionalmente supone que el término "secreto" ha sido definido en otra política.

Políticas Relacionadas: “[Clasificaciones de Medios de Almacenamiento de Datos](#)” y “[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

7. Cubrir Información Sensible

Política: Todos los trabajadores que manejen información secreta, confidencial o privada de la Empresa X, deben ocultar esta información de personas no autorizadas que estén en los alrededores.

Comentario: Esta política instruye a los usuarios en el sentido de que deben ocultar la información sensible cuando se les interrumpe en su oficina o sitio de trabajo. Si ellos actúan como está descrito en esta política, los trabajadores evitarán que la información sea vista por personas no autorizadas, a pesar de que las personas que interrumpen son normalmente también empleados. Un efecto secundario positivo está representado por los reclamos de las personas que consideran que es difícil trabajar de esta manera. Por ejemplo, una recepcionista encontrará difícil manejar información sensible al mismo tiempo que atender a los visitantes. En vez de indicar una deficiencia en la política, este reclamo indica que el trabajo que realiza una persona en información sensible es incompatible con sus deberes como recepcionista. Como solución, la persona puede efectuar su trabajo en un sistema de computación ubicado en una oficina privada cuando no esté

efectuando trabajos de recepcionista. Esta política supone que los términos "secreto, confidencial y privado" han sido definidos en otra política.

Políticas Relacionadas:“[Clasificación de Datos en Cuatro Categorías](#),” “[Áreas Desatendidas](#),” “[Comunicaciones Potencialmente Ofensivas](#),” y “[Sesiones Activas Desatendidas](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

8. Gabinetes de Archivo con Llave

Política: Todos los trabajadores de oficina deben recibir archivadores con llave, donde todo el material sensible se debe guardar al retirarse los trabajadores de su escritorio, y una copia de la llave del gabinete debe ser entregada al gerente del departamento.

Comentario: Esta política garantiza que los trabajadores estarán dotados con una de las herramientas básicas para conservar la confidencialidad de los datos. La política también notifica a la gerencia local que debe suministrar este tipo de muebles a todos los trabajadores de oficina. La política requiere que los empleados usen estos archivadores con llave para guardar material confidencial. La palabra "confidencial" tendrá que ser definida en otra parte, quizás en una política de clasificación de datos. Si los trabajadores pierden u olvidan la llave, el gerente del departamento tiene una llave de respaldo. En algunos casos, también se deberían depositar llaves de respaldo con el gerente de seguridad física.

Políticas Relacionadas:“[Llaves de las Estaciones de Trabajo](#),” “[Escritorios Limpios — Uso Activo](#),” y “[Requisitos de Seguridad para Teletrabajo](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

7.03.02 Remoción de Propiedades

1. Pases de Propiedad

Política: A menos que tengan un pase autorizado, las máquinas de escribir, los teléfonos celulares, los computadores portátiles, el equipo de modem y todo lo relacionado con sistemas informáticos, no deben salir de las instalaciones de la Empresa X.

Comentario: Esta política garantiza que los trabajadores no están robando equipos o la información almacenada en ellos. Guardias en los puntos de salida pueden revisar los pases para asegurarse que están vigentes, aprobados por la gerencia y que se refieren al equipo correspondiente. Esta política es particularmente importante para computadores personales y estaciones de trabajo. Se requiere un pase tanto para la propiedad personal como para la propiedad de la Empresa X. La nueva tecnología

activará alarmas en puntos controlados en las entradas y salidas del edificio si el equipo que está siendo removido, ha sido etiquetado. El proceso de pases puede ser un método para evitar que estas alarmas se activen. Esta política puede ser ampliada para prohibir a los visitantes, personal temporal y familiares de empleados remover cualquier equipo de las instalaciones de la Empresa X.

Políticas Relacionadas: “Acceso Físico para Terceros” y “Traslado de Equipos de Computación de Oficinas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Etiquetas Anti-Robo

Política: La información sensible de la Empresa X no se debe almacenar o cargar en ningún aparato de computación portátil, a menos que los aparatos porten una etiqueta electrónica de seguridad autorizada.

Comentario: Esta política disuade a los trabajadores de almacenar o cargar información en aparatos de computación portátil. Si los usuarios deben almacenar o cargar información sensible en aparatos portátiles, no solamente deben usar controles de acceso criptográficos y rigurosos, sino que cada aparato debe estar etiquetado para que su remoción del edificio sea detectada por un guardia, y se evite la remoción del aparato. Esta política será más efectiva si el edificio tiene una trampa humana o torniquete a través del cual las personas deben pasar para salir del edificio. La política hace uso de la misma tecnología utilizada por tiendas por departamento para detectar el robo de ropa y otros bienes. La política reconoce que hay usos legítimos para computadores portátiles que pueden contener información sensible. Pueden utilizarse pases para legitimar la remoción de tales dispositivos portátiles de los edificios controlados.

Políticas Relacionadas: “Viajes con Información Secreta” y “Remoción de Información Sensible en Papel”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

3. Traslado de Medios

Política: Todo medio de almacenamiento de computación que salga de la Empresa X debe estar acompañado de un pase autorizado, el cual debe registrarse en la recepción del edificio.

Comentario: Esta política garantiza que los trabajadores no se están llevando información sensible o valiosa. Los primeros riesgos que esta política trata de contrarrestar son el espionaje industrial, la violación de la propiedad, el robo de propiedad intelectual y el sabotaje. La política puede ser difícil para organizaciones que tengan un contingente numeroso de teletrabajadores, muchos de los cuales por costumbre cargan medios de almacenamiento y con ellos entran y salen de las oficinas del edificio. Los discos duros de computadores portátiles son también medios de almacenamiento y también deben tener pases o permisos. Esta política es apropiada para ambientes de alta seguridad, tales como embajadas diplomáticas, un centro de procesamiento de datos de un banco o un puesto de comando militar.

Políticas Relacionadas: “Pases de Propiedad” e “Inspección de Bolsos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

8 GESTIÓN DE OPERACIONES Y COMUNICACIONES

8.01 Responsabilidades y Procedimientos Operativos

8.01.01 Procedimientos Operativos Documentados

1. Procesos, Sesiones y Archivos de Usuarios

Política: El personal de administración de sistemas de la Empresa X puede, en cualquier momento y sin previo aviso, alterar la prioridad o concluir la ejecución de cualquier proceso del usuario que crea consume recursos excesivos del sistema, o que está degradando significativamente el tiempo de respuesta del sistema, concluir las sesiones del usuario o conexiones si estima que este uso infringe las políticas de seguridad o consume recursos excesivos del sistema, o remover o comprimir los archivos del usuario si cree que estos archivos consumen espacio excesivo en el disco.

Comentario: Esta política notifica a los usuarios acerca de las actividades de los administradores del sistema y evita algunos reclamos. La política también notifica a los usuarios que el personal de administración de sistemas tienen una gran amplitud para inmediatamente manejar cualquier cosa que crean pueda poner en riesgo la disponibilidad, integridad o seguridad del sistema. La política actúa como elemento disuasivo ante actos abusivos, como ejecutar juegos en los sistemas de la Empresa X, especialmente juegos multiusuario que consumen una gran cantidad del ancho de banda de la red.

Políticas Relacionadas: “[Consumo de Recursos por Programas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Registros de Aplicaciones Críticas

Política: Todas las aplicaciones críticas del negocio deben ser apoyadas mediante registros que permitan que las actividades del sistema se reanuden dentro de 15 minutos.

Comentario: Esta política notifica a la gerencia de Sistemas Informáticos y a las organizaciones usuarias que manejan sus propios sistemas, que las aplicaciones críticas deben ser recuperadas dentro de cierto período de tiempo y que los registros extensos juegan un papel importante en el proceso de restauración. La especificación de un cierto período de tiempo para restaurar

hace relativamente fácil que las personas determinen si están cumpliendo o no la política. El período de tiempo varía dependiendo de la organización, e idealmente se debe basar en un análisis del impacto sobre el negocio. El período de tiempo también es una función de la criticidad de la información manejada por la aplicación correspondiente. Los registros utilizados para la recuperación pueden tener la forma de bases de datos replicadas, puntos de control de bases de datos, fotografías de archivos, discos espejos u otros. En las anotaciones explicativas que acompañan a esta política pueden aparecer referencias a este tipo de registros a pesar de que muchas veces es mejor mantener los detalles técnicos fuera de la política. El período específico de tiempo también puede ser mencionado fuera de la política porque es probable que cambie con el tiempo.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Clasificación de la Criticidad de las Aplicaciones Multiusuario](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

3. Documentación de las Aplicaciones de Producción

Política: Antes de mover la aplicación hacia un ambiente de producción, el Propietario correspondiente de la información debe haber preparado y autorizado la documentación para todas las aplicaciones de producción, lo cual incluye una lista de los recursos de sistemas que deben ejecutarse, una lista de los archivos utilizados y afectados, una lista de los aspectos de seguridad, una descripción de las formas en que el flujo de trabajo se va a monitorear y gerenciar, y una descripción de la forma de cómo será manejado el producto resultante.

Comentario: La política evita que las aplicaciones desarrolladas internamente se lleven a producción sin la documentación adecuada sobre las operaciones de computación. La política se pudiera abreviar cuando la lista que detalla los tipos de documentación requeridos se encuentra en otro documento. Esta política no debe ser confundida con una similar que se refiere a la documentación de la programación codificada por un

usuario final. Esta política se refiere a aplicaciones que serán gerenciadas por un departamento de Tecnología Informática.

Políticas Relacionadas: “Convenciones en Desarrollo de Sistemas” y “Adiestramiento en Seguridad Informática”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Disponibilidad del Sistema

Política: Los usuarios deben ser capaces de acceder a todos los sistemas computarizados compartidos por lo menos 95% de las horas normales de trabajo, calculado sobre una base mensual.

Comentario: La intención de esta política es hacer que la alta gerencia evalúe qué tipo de disponibilidad de sistema se necesita en la organización. Si bien el porcentaje puede cambiar con el tiempo, hay méritos suficientes para definirlo como un requerimiento. Pueden derivarse de esta política esfuerzos específicos de planificación de contingencias y decisiones de diseño de sistemas, pero el porcentaje exacto especificado será una función de las propias necesidades de la organización. El porcentaje que se da aquí puede ser aceptable para una compañía manufacturera, pero puede ser no aceptable para una compañía telefónica. Una política de este tipo también puede ser útil para asuntos de contratación externa, solicitudes de propuestas y otras interacciones con terceros. La política es una forma de convenio a nivel de servicio.

Políticas Relacionadas: “Planes de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Planes de Recuperación Ante Desastre Computacional

Política: La gerencia debe preparar, periódicamente actualizar y regularmente probar un plan de recuperación de desastres que permita que todos los sistemas críticos de computación y comunicación estén disponibles en el evento de una pérdida mayor, tales como los causados por inundación, terremoto o tornado.

Comentario: Esta política requiere que la gerencia preste apoyo financiero y atención esmerada a los esfuerzos de planificación de contingencias ante

desastres. Como los desastres ocurren raras veces, la gerencia técnica a menudo ignora los procesos de planificación para recuperarse de los desastres. Estos gerentes están cambiando su actitud sobre los planes de recuperación de desastres, principalmente debido a que reconocen que tener un buen plan de contingencia se convierte en una ventaja competitiva. La gerencia está comenzando a apreciar que el desempeño en el trabajo está mayormente basado en la atención que se le preste a estos asuntos. El enfoque de esta política es en desastres, a pesar de que es recomendable tener una política que se ocupe de otro tipo de interrupciones. Esta política asume que el término "crítico" ha sido definido en otra parte. Los desastres naturales específicos mencionados en esta política pueden ser adaptados a las condiciones locales. Esta política no está limitada a desastres naturales, sino que se aplica a cualquier evento que resulte en una pérdida extendida de la disponibilidad del sistema.

Políticas Relacionadas: “Planes de Respuesta Ante Emergencias Computacionales,” “Preparación y Mantenimiento de Planes de Contingencia Empresarial,” “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” y “Planes de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

6. Puestos Técnicos Esenciales

Política: La gerencia debe preparar anualmente un inventario de las posiciones técnicas esenciales de la Empresa X y los nombres de los individuos que actualmente las ocupan.

Comentario: Esta política destaca el peligro de depender de ciertas personas y fomenta el adiestramiento cruzado, la rotación de posiciones, el desarrollo de expertos en sistemas y otras formas de suministrar cierta redundancia para personas clave. En las corporaciones grandes, el departamento de gestión de riesgo elabora inventarios similares. En los círculos empresariales, los reemplazos y los nuevos cargos para gerentes de alto nivel que no pueden seguir desempeñando sus cargos es un tópico frecuente de conversación. Este mismo procedimiento puede y debe ser aplicado al personal técnico crítico, tales como las personas mayores que programan comutadores en compañías telefónicas. Como resultado del inventario, la gerencia en muchos casos concluirá que no tiene suficiente

personal técnico suplente. El proceso de identificar las aplicaciones críticas, en algunos casos, puede ayudar a enfocar la atención en el personal técnico clave.

Políticas Relacionadas: “Adiestramiento Multidisciplinario,” “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” e “Inventario de Activos — Tecnología”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

7. Adiestramiento Multidisciplinario

Política: En todo momento, por lo menos dos miembros del personal deben estar en capacidad de prestar cualquier servicio técnico esencial para los sistemas informáticos críticos de la Empresa X.

Comentario: Esta política garantiza que si un técnico que presta servicios básicos no estuviera disponible en algún momento, esto no significaría entonces que los sistemas empresariales críticos se paralizarían, existiendo varios métodos gerenciales para remediar esta eventualidad. Por lo tanto, la empresa puede ser creativa en cuanto a reducir su dependencia de una sola persona. Esta política también se aplica a aquellas situaciones en las cuales la empresa desea disminuir su nivel de exposición y no cuenta entre su personal con alguien que preste los servicios técnicos básicos. Un ejemplo sería que la empresa decidiera mantener parte de sus documentos operacionales al día. Las acciones impuestas por esta política podrían ser obviadas si la empresa determina que ciertos servicios técnicos no son indispensables; de ser así, e independientemente de que algunos empleados piensen que sí lo son, se puede evidenciar que la empresa consideró seriamente la situación. Esta política asume que ciertos sistemas informáticos han sido definidos previamente como críticos o indispensables. También asume que la Empresa X es una organización con un número adecuado de personal, y que se puede permitir cierta redundancia con el personal. Aquellas organizaciones de menor escala deberán ser más creativas, tal vez designando un consultor técnico ambulante a cambio de un pago fijo de poca cuantía.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Puestos Técnicos Esenciales,” “Pericia en Sistemas,” “Empleados Que Viajan Conjuntamente,” y “Documentación para Sistemas de Producción”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Información de Contacto

Política: Todos los integrantes del departamento de Sistemas informáticos que viajan fuera de la ciudad, deben hacer uso de un buscaperonas y proporcionar tanto al gerente como a la secretaria del grupo de trabajo, los números telefónicos donde puedan ser localizados en cualquier momento después de las horas hábiles y mientras se encuentren de viaje.

Comentario: Esta política demuestra la gran confianza depositada en el personal encargado de los sistemas informáticos. La intención de esta política es la de mantener la habilidad de contactar rápidamente a todo el personal técnico necesario en caso de siniestro o emergencia. Dicha política puede ser extendida a los miembros de los departamentos usuarios que estén involucrados en asuntos técnicos computacionales y comunicacionales, así como a aquellos proveedores de los que depende la empresa. La política se aplica a una diversidad de trabajadores, inclusive a aquellos que se encuentren en vacaciones o asistiendo a conferencias, así como también a los días feriados y otras horas no hábiles. Posiblemente algunas empresas no requerirán una política tan global, sino lo suficiente como para asegurar que todos los programadores de sistemas, los programadores de aplicaciones y los especialistas en redes informáticas estén disponibles a través de sus buscaperonas. Desafortunadamente, algunas veces el personal técnico viaja a ciertos lugares donde no funcionan los buscaperonas, y estas situaciones son las que hacen necesario el proporcionar números telefónicos adicionales tanto al gerente como a la secretaria. Aquellas organizaciones que ameriten estar en contacto permanente con miembros del personal técnico indispensable, querrán reemplazar la palabra “buscaperonas” por “teléfono celular”

Políticas Relacionadas: “Equipo de Respuesta Ante Emergencias Computacionales” y “Empleados Que Viajan Conjuntamente”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Cambios en Producción

Política: Los datos de producción y los programas informáticos de producción de la Empresa X deben ser modificados sólo por el personal autorizado y de acuerdo con los procedimientos establecidos.

Comentario: Esta política garantiza que se utilizan controles especiales en la protección de la integridad de los datos y los programas de producción de la Empresa X. Se garantiza una atención especial a la seguridad de estos datos y programas ya que los mismos se utilizan en actividades empresariales críticas. Generalmente, serán pocas las personas autorizadas y las autorizaciones se otorgarán si y sólo si tales personas demuestran necesitar estos privilegios. Un sistema de control de cambios formal o un sistema de gestión de cambios pudiera utilizarse para automatizar y llevar el seguimiento de los cambios y las autorizaciones asociadas. Las autorizaciones pueden implementarse a través de contraseñas, tarjetas inteligentes, firmas digitales, certificados digitales, cifrado, firmas autógrafas y otros métodos. Los programas informáticos pueden considerarse un tipo especial de datos informáticos. Para que un entorno informático esté seguro, tanto los datos como los programas informáticos necesitan controles de cambios.

Políticas Relacionadas: “Procedimiento de Control de Cambios” y “Ordenes para Cambiar Registros”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

10. Autorización para Transacciones de Producción

Política: Las transacciones que actualicen registros empresariales deben procesarse sólo si han sido autorizadas por la gerencia de la Empresa X.

Comentario: Esta política garantiza que sólo aquellas transacciones debidamente autorizadas podrán actualizar los registros de producción aun cuando éstos estén computarizados. La política también podrá extenderse con el fin de especificar lo que significa autorización, lo cual generalmente significa una delegación clara de poder de decisión, además de la aprobación por parte de la gerencia de llevar a cabo ciertas acciones. Los controles de acceso informáticos basados en contraseñas representan las formas más frecuentes de verificar si alguien está o no autorizado para realizar una transacción. De todas maneras, esta política está definida de tal forma que el proceso de autorización pudiera incluir también una firma autógrafa sobre un documento escrito.

Políticas Relacionadas: “Autorización para Transacciones en Sistema de Producción” y “Actualización de Información de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Corrección de Registros de Negocios

Política: Cualesquier registros errados de la Empresa X que existan deben ser corregidos inmediatamente utilizando los procedimientos de control establecidos.

Comentario: Esta política requiere que se utilicen los procedimientos de control establecidos para actuar sobre las modificaciones relacionadas con corrección de errores de los registros empresariales de la Empresa X. Estos procedimientos de control pueden incluir el obtener una autorización gerencial antes de llevar a cabo una modificación, o realizar modificaciones mediante una modalidad de separación de tareas con otro trabajador. Es importante definir las restricciones sobre quiénes pueden realizar modificaciones correctivas a los registros empresariales, y así evitar que alguien cometa una estafa, sabotaje u otro tipo de acciones no autorizadas. El hecho de estar en conocimiento de que los registros no están correctos no es suficiente, por lo que deben ser corregidos continuamente y así mantener la integridad de la información. También se encuentra implícito en esta política que no debe conservarse una colección separada de libros que no describan la situación actual de la empresa. Tenemos por ejemplo, que una colección de libros de apariencia engañosa podría ser conservada para atender los asuntos relacionados con los inversores, mientras que una colección de libros más realista puede ser conservada para dar información a los más íntimos. Esta política no previene o trata de disuadir a una organización de conservar diferentes colecciones de libros para objetivos diferentes, siempre que dichos libros conserven los procedimientos normales. Por ejemplo, esto podría incluir una colección de libros para fines impositivos y otra colección de libros para fines contables.

Políticas Relacionadas: “Investigación de Errores,” “Normas de Implementación de Controles,” y “Separación de Tareas”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

12. Pericia en Sistemas

Política: Se debe contar con por lo menos dos personas disponibles con pericia en asuntos críticos de informática y comunicaciones.

Comentario: Esta política evita que una organización se encuentre en la engorrosa situación de no contar con el personal idóneo para proporcionar asistencia técnica. Esto podría suceder, a manera de ejemplo, cuando un terremoto causa daños a un centro de procesamiento de datos, y fallece un programador indispensable de los sistemas cliente-servidor. Desde el punto de vista de que nadie más en la organización cuenta con el conocimiento que tal programador poseía, podría retrasarse de manera significativa la recuperación de los sistemas de producción que se encuentren fuera de las instalaciones. La política no expresa en forma explícita que el personal que goza de la mayor pericia debe ser un empleado permanente; éstos bien podrían ser contratistas o consultores. En este sentido, la palabra relevante dentro de esta política es "disponibles". De igual manera, la política respalda el desarrollo y el mantenimiento de una base de datos que contenga toda la información relacionada con las competencias que posean tanto los empleados como el personal restante de una organización. Indirectamente, la política implica que la gerencia debe definir cuales áreas son las más importantes. Esto fomenta una concientización de los posibles riesgos en que se pueda incurrir, especialmente en aquellos relacionados con planes de contingencia. Algunas organizaciones preferirían utilizar la palabra "crítico" en vez de "importante"; de igual manera, cualquiera de los siguientes términos, "crítico para la misión" o "estratégico", podrían ser utilizados en vez de "importante"

Políticas Relacionadas: ["Adiestramiento Multidisciplinario"](#) y ["Sistemas de Seguridad Independientes"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8.01.02 Control de Cambios Operacionales

1. Identificadores de Usuarios Privilegiados Suministrados por Proveedor

Política: Previo a la instalación de un sistema operativo informático multiusuario en la Empresa X, el personal técnico debe desactivar o renombrar todos los identificadores de usuarios privilegiados, tales como aquellos denominados "administrador", "auditor" o "instalador".

Comentario: Los identificadores privilegiados de usuario proporcionados por proveedores son el objetivo de muchos ataques, tales como los de intentos de adivinar la contraseña. Al eliminarlos o renombrarlos, el personal técnico de la Empresa X impide que se

13. Facturas por Servicios Computacionales y Comunicacionales

Política: Los usuarios de computadores deben revisar inmediatamente los detalles de sus facturas por uso de servicios informáticos y comunicacionales, inclusive de informes internos de recargo, para asegurarse de que los cobros son correctos, que no se han cometido errores de importancia y que no se ha incurrido en un uso significativo no autorizado.

Comentario: Esta política requiere que los gerentes del departamento de usuarios revisen sus facturas para que determinen rápidamente usos no autorizados y otros errores relacionados con la seguridad informática. Las facturas a las cuales se refiere la presente política podrían ser las de la asociación de servicios informáticos, las detalladas del sistema telefónico de larga distancia o las de los informes de contabilidad interna por recargos. La política no establece diferencias entre proveedores de servicios informáticos o comunicacionales propios o extraños. La política es muy importante de manera particular para los operadores telefónicos privados, los cuales pueden acumular rápidamente facturas por montos importantes sobre llamadas no gratuitas y no autorizadas. Algunas organizaciones podrían también extender el alcance de esta política a las facturas de las tarjetas de crédito.

Políticas Relacionadas: ["Partida Presupuestaria para la Seguridad Informática"](#) e ["Implantación del Acceso al Sistema Telefónico Directo"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

convirtan en el objetivo de estos hackers. Tal como está definida, la política resulta efectiva contra algunos ataques automatizados, pero para hacer el proceso de renombramiento más eficaz, puede modificarse especificando que los nombres de los identificadores de usuario nuevos no guarden relación alguna con los nombres anteriores. A manera de ejemplo, el identificador del usuario "auditor" no puede ser renombrado "auditorEDP". Para mayor seguridad, la palabra "multiusuario" puede ser eliminada de la política, lo que haría a la política aplicable a computadores personales de escritorio.

Políticas Relacionadas:“Controles de Acceso al Sistema de Computación”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

2. Remoción de Software

Política: Todo módulo o utilidad del sistema operativo que definitivamente no ha de utilizarse, y que no sea necesario para el funcionamiento de otro software esencial del sistema, debe ser eliminado o desactivado antes de ser utilizado con la información de producción.

Comentario: Esta política impide que tanto los hackers como cualquier otra persona puedan utilizar las rutinas de software de los sistemas, innecesarias para la actividad empresarial con la idea de poder entrar sin autorización al sistema. Mientras menor sea el número de utilidades dentro de un sistema en particular, menos vías de ataque habrá para un hacker o cualquier otro tipo de adversario. Recientemente, muchos fabricantes han recargado el software de sus sistemas con funciones adicionales, innecesarias para la gran mayoría de las organizaciones usuarias, pero muy útiles para un intruso. De manera indirecta esta política establece que todo software innecesario debe ser eliminado de los sistemas de producción. Puede ser difícil implementar esta política ya que varios proveedores no desean que el personal técnico de los usuarios altere las aplicaciones o los sistemas operativos, y no proporcionan instrucciones para la remoción o desactivación segura de los módulos o utilidades innecesarios. Reducir la cantidad de paquetes de software del sistema de producción también disminuye potencialmente la necesidad de mantenimiento. El enfoque de esta política es ampliamente utilizado en los cortafuegos y en los servidores comerciales de Internet, los cuales utilizan este planteamiento en el desarrollo de software de sistemas. Lo previsto en esta política no impide que el software eliminado sea reinstalado, de ser necesario. La política tampoco establece cómo determinar si ciertos paquetes de software serán solicitados y si se requerirá cierto nivel de investigación. Algunas organizaciones pueden especificar esta información, así como sobre quién recae la responsabilidad de tomar la decisión final por efecto de la política.

Políticas Relacionadas:“Almacenamiento de Utilidades del Sistema” y “Uso de las Utilidades del Software del Sistema”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

3. Cambios del Sistema Operativo de Producción

Política: Las extensiones, modificaciones o sustituciones al software de los sistemas operativos de producción, sólo pueden ser llevadas a cabo si se ha recibido previamente una autorización escrita por parte del gerente del departamento de Seguridad Informática.

Comentario: Esta política disuade y controla de manera estricta cualquier modificación en los sistemas operativos informáticos de producción. Como regla general, es aconsejable mantener como norma un sistema operativo proporcionado por un proveedor. Esto se debe a que los cambios en el software de los sistemas operativos pueden introducir de manera imperceptible ciertas vulnerabilidades. El mantener sistemas operativos modificados puede resultar sumamente oneroso, tanto en tiempo como en dinero. Los sistemas operativos personalizados, o simplemente incompatibles, pueden interferir seriamente en la conexión de los computadores a las redes. Si las modificaciones en los sistemas operativos han sido cuantiosas, las organizaciones pueden verse limitadas en sus intentos de migrar a las nuevas versiones de los sistemas operativos o de los programas de aplicaciones. Esto también pudiera significar que la organización no puede utilizar los nuevos arreglos de seguridad incorporados a la nueva versión de un sistema operativo. En las organizaciones técnicamente sofisticadas, esta política puede distribuirse en forma apropiada a los usuarios finales.

Políticas Relacionadas:“Versiones de Sistemas Operativos” y “Uso de las Utilidades del Software del Sistema”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

4. Revisiones de los Cambios al Sistema Operativo de Producción

Política: Deben llevarse a cabo revisiones periódicas o evaluaciones de la vulnerabilidad de los sistemas operativos de producción.

Comentario: Debido a que varias funciones de control del acceso son implementadas a nivel de sistema operativo, o a nivel del paquete de control del acceso, es importante garantizar que se han efectuado sólo modificaciones autorizadas al sistema operativo. Los sistemas operativos juegan un papel absolutamente crítico en la seguridad, y por ello deben ser validados periódicamente a través de una revisión, tal vez a través de un programa de comparación de archivos o tal vez a través

de firmas digitales. Esta política exige dicha revisión. Una política que especifique la necesidad de tal revisión es importante ya que muchas veces las organizaciones no cuentan con la pericia técnica propia para llevar a cabo tal revisión. Ahora es más frecuente que dichas revisiones se realicen mediante paquetes de software. En ambientes de computadores personales, de cliente-servidor y de redes de área local, podrían utilizarse de manera periódica tanto el software de manejo de licencias que incluya sumas de verificaciones como el software antivirus, para implementar esta política. El lector podría decidir incluir "sistemas operativos de servidores en redes" y "sistemas operativos de cortafuegos" como parte de la política.

Políticas Relacionadas: "Cambios del Sistema Operativo de Producción"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Versiones de Software

Política: Todos los sistemas operativos de producción de la Empresa X, los sistemas de administración de bases de datos, los cortafuegos y el software relacionado, así como todo el software de aplicaciones de negocios de producción, deben mantenerse en su versión más reciente y más estable.

Comentario: Esta política gira instrucciones al personal de operaciones informáticas sobre la actualización del software residente en los sistemas de producción. Todos los sistemas operativos, los cortafuegos y los sistemas de administración de bases de datos juegan un papel importante en el área de seguridad. De igual manera, el software de aplicaciones incluye de manera frecuente sus propios mecanismos de seguridad, tales como contraseñas o restricciones a los privilegios. La versión más reciente del software incluye las correcciones de las vulnerabilidades de seguridad conocidas, y proporciona a la organización usuaria un nivel de seguridad superior al que puede obtenerse con otras versiones. Se incluye la palabra "estable" en la política con el fin de impedir que la organización usuaria sea un sitio de prueba, si ésa no era su intención original. Los niveles de las versiones son diferentes de los parches y las correcciones.

Políticas Relacionadas: "Arreglos de Seguridad," "Sistemas en Interface con Redes Externas," y "Versiones de Sistemas Operativos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Procedimientos de Retorno

Política: Deben desarrollarse procedimientos adecuados de rectificación que permitan que las actividades de procesamiento de información se reviertan rápida e inmediatamente a las condiciones previas a la modificación más reciente de software, en todas las modificaciones realizadas en el software de los sistemas de producción y en las aplicaciones de producción.

Comentario: Dada la naturaleza compleja e interconectada de los sistemas informáticos, la empresa puede verse en problemas si solicita una conversión a un nuevo sistema sin procedimientos de rectificación bien definidos. En aras de mantener los sistemas de producción en marcha el mayor tiempo posible, esta política garantiza que el procesamiento de negocios no se verá interrumpido, porque cuenta con una versión confiable y estable del software de producción. Esta política es de especial importancia en ambientes cliente-servidor y en otros ambientes complejos donde las aplicaciones abarcan desde múltiples sistemas operativos, múltiples ubicaciones y múltiples tamaños de computadores. En estas circunstancias, puede que no sea suficiente ir a una versión anterior de una aplicación, porque muchas otras cosas pueden haber cambiado también.

Políticas Relacionadas: "Planes de Contingencia en Conversión de Software"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Versiones de Sistemas Operativos

Política: Una vez se compruebe que el software es estable, la Empresa X debe utilizar la versión más reciente del sistema operativo en computadores multiusuario.

Comentario: Si se quiere instalar la última versión de un sistema operativo, se recomienda que la empresa se tome su tiempo, a menos que tenga la intención de descubrir y arreglar los errores de las nuevas versiones. Esta política garantiza que la organización ha implementado las versiones más recientes de los sistemas operativos porque ya incluyen varias correcciones de seguridad, y cuenta ahora con la mayor seguridad en sistemas operativos. La política podría ser ampliada para incluir sistemas operativos de redes. La óptima seguridad del sistema operativo es fundamental para tanto la óptima seguridad del sistema de administración de bases de datos como para la óptima seguridad de las aplicaciones. Una deficiencia en la seguridad del

sistema operativo podría socavar los controles sofisticados que se encuentran en la base de datos o en las aplicaciones.

Políticas Relacionadas: “Cambios del Sistema Operativo de Producción,” “Madurez del Producto de Seguridad,” “Herramientas y Técnicas de Desarrollo Maduras,” y “Arreglos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8.01.03 Procedimientos de Gestión de Incidentes

1. Arreglos de Seguridad

Política: Debe instalarse con prontitud todo el software de seguridad suministrado por los proveedores de sistemas operativos, por los equipos oficiales de respuesta ante emergencias computacionales y por otros terceros confiables.

Comentario: El objetivo de esta política es indicar a los gerentes de sistemas que deben instalar lo antes posible, todas las correcciones de seguridad. Los proveedores usualmente esperan hasta que un problema ya no pueda ser ignorado para utilizar un corrector de seguridad, lo que significa que la organización debe implementar lo antes posible sus correctores de seguridad para prevenir cualquier pérdida. Si bien la intención es que la política se aplique solamente a sistemas operativos, su alcance podría ser ampliado para incluir también las aplicaciones, las utilidades del sistema y otros tipos de software. El alcance de la política también podría ser ampliado para incluir otras organizaciones de confianza tales como grupos usuarios, además de los equipos de respuesta ante emergencias computacionales. La política apoya también la necesidad de los gerentes de sistemas de contar con las últimas versiones del software para los sistemas operativos. La implantación de esta política puede hacerse mediante la distribución automática de software a través de una red, en particular para sistemas cliente-servidor, redes de área local, computadores personales y a través de medios tradicionales de distribución, como la cinta magnética y los CD-ROM.

Políticas Relacionadas: “Versiones de Sistemas Operativos” y “Responsabilidades en el Manejo de Incidentes”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Planes de Respuesta Ante Emergencias Computacionales

Política: La gerencia debe preparar, actualizar periódicamente y poner a prueba planes de contingencia informática que permitan una operación continua de los sistemas críticos en caso de interrupción o en caso de degradación del servicio.

Comentario: Esta política requiere que la gerencia prepare, actualice y ponga a prueba planes de contingencia adicionales a los planes de respuesta a siniestros. La referencia a “degradación del servicio” podría ser omitida sin afectar en mayor grado a la política. En algunas organizaciones, tales como las agencias gubernamentales civiles y en otros entornos no competitivos, no se da mayor importancia a la degradación del servicio. De igual manera, para que esta política tenga una mayor eficacia, el término “crítico” tendría que haber sido definido con anterioridad.

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones” y “Planes de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Equipo de Respuesta Ante Emergencias Computacionales

Política: La gerencia debe organizar y mantener un equipo propio de respuesta ante emergencias computacionales que suministre la identificación acelerada de los problemas, el control de daños y servicios de corrección de los problemas en caso de emergencias informáticas, tales como infecciones de virus o ataques de hackers.

Comentario: Los equipos de respuesta ante emergencias computacionales (CERT, por sus siglas en inglés) externos y confiables asisten a los usuarios en la Internet, mientras que otros CERT coordinan las investi-

gaciones y los esfuerzos para erradicar problemas internacionales. Más allá de estos CERT multiorganizacionales, existe la necesidad de un CERT propio de la empresa que maneje los problemas que allí se presentan. Mediante la designación formal de un CERT dentro de la empresa, la organización se encuentra en mejor posición para manejar contingencias relacionadas con la seguridad. El uso de un CERT dentro de la empresa también reduce la posibilidad de que los problemas se hagan del conocimiento público. Esta política requiere que la gerencia del departamento de Tecnología Informática establezca y respalde un CERT.

Políticas Relacionadas: “Presentación de la Imagen Pública,” “Informes de Violaciones y Problemas,” “Responsabilidades en el Manejo de Incidentes,” “Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio,” y “Sistema de Alerta de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4. Simulacros del Equipo de Respuesta Ante Emergencias Computacionales

Política: Por lo menos una vez cada tres meses, el departamento de Seguridad Informática debe utilizar simulacros para movilizar y probar el Equipo de Respuesta ante Emergencias Computacionales de la Empresa X.

Comentario: Esta política requiere que los simulacros del Equipo de Respuesta para Emergencias Informáticas (CERT, por sus siglas en inglés) se realicen con cierta frecuencia. Si la gerencia especifica una frecuencia mínima para estas pruebas, la misma asegurará que no van a ser ignoradas a favor de otras actividades de negocios urgentes. La política garantiza que un CERT interno funciona eficiente y eficazmente. Si el CERT no opera de esta manera, la situación será evidenciada por un simulacro fallido. El alcance de la política podría expandirse con el fin de solicitar un informe de una página con los resultados de las pruebas y que éstos sean enviados al gerente de informática o algún otro ejecutivo de nivel medio. Esta política asume que ya existe un CERT y que está dotado con el personal adecuado.

Políticas Relacionadas: “Arreglos de Seguridad” y “Equipo de Respuesta Ante Emergencias Computacionales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Sospecha de Intrusión en los Sistemas

Política: Cada vez que se sospeche que un sistema está comprometido, el computador involucrado debe ser desconectado inmediatamente de todas las redes, y deben seguirse todos los procedimientos necesarios para asegurar que el sistema no está comprometido antes de re conectarlo a la red.

Comentario: Esta política garantiza que el computador comprometido no podrá utilizarse para influenciar ningún otro computador de la red y que se seguirán una serie de procedimientos predefinidos para que el sistema retorne a un nivel de seguridad previo a su reconexión a la red. Incluidos en estos procedimientos deberían estar el ejecutar un software de comparación de archivos que identifique modificaciones recientes, la ejecución de procedimientos de investigaciones forenses, la restauración del software de sistemas a partir de copias de respaldo confiables, la re-inicialización del sistema de control del acceso y el copiado del registro del sistema vigente en otros medios de almacenamiento que estén bajo llave. Los administradores de sistemas frecuentemente reciben presión de los administradores de usuarios para que no se desconecten de las redes internas, que no verifiquen si los archivos han sido modificados, y que no se tomen el tiempo en re establecer un sistema de control de acceso confiable. Esta política hace caso omiso a los deseos de los administradores usuarios, exigiendo la ejecución de estos pasos esenciales. Un procedimiento que puede ser añadido es el uso de una firma digital aplicada al registro del sistema almacenada en un contenedor fuera de línea. Esto podría ser utilizado más adelante en el tribunal para resaltar la integridad de la evidencia registrada. Esta política garantiza que los intrusos ya no estarán conectados. Si la máquina no sale de la red, los intrusos pudieran estar observando e interfiriendo con las actividades de recuperación.

Políticas Relacionadas: “Cambios de Contraseña Luego de Estar Comprometido el Sistema,” “Apagado de Computadores,” y “Período de Retención de Registros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Procedimientos de Respuesta a Intrusión

Política: Todo el personal de operaciones computacionales debe tener un procedimiento documentado vigente que especifique claramente cómo se manejarán los incidentes de seguridad informática.

Comentario: Esta política está motivada por la situación en la cual el personal de operaciones informáticas sabe que está ocurriendo un ataque, pero no sabe qué hacer, o a quien contactar. Como resultado, el hacker procede y ocasiona daños importantes, cuando pudo haber sido detenido, registrado, rastreado, disuadido o manejado oportunamente. Toda vez que esta política está orientada hacia aquellos que gestionan servidores comerciales, servidores web, servidores de bases de datos, y otras máquinas multiusuario, también podría aplicarse a aquellos individuos no reconocidos como integrantes del grupo de Operaciones del departamento de Sistemas Informáticos. El personal técnico de los departamentos usuarios que vela por los sistemas de producción, podría ser considerado personal de operaciones computacionales si la organización aprueba la definición de "personal de operaciones computacionales" de una manera amplia e incluyente. Este procedimiento documentado especificaría los tipos de incidentes que cubre el documento, quién y cuándo debe ser notificado, qué debe hacerse después de que ocurre un incidente, cómo debe protegerse la evidencia, tales como los registros, cómo limitar los daños inmediatamente, cómo evitar problemas futuros de esta naturaleza, cómo reestablecer un entorno confiable en los sistemas informáticos y cómo documentar las acciones que se llevaron a cabo para responder al incidente.

Políticas Relacionadas: ["Revisión de Registros del Sistema,"](#) ["Sistemas de Detección de Intrusos,"](#) y ["Verificación de la Integridad del Sistema"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Alertas Sobre Vulnerabilidades

Política: Sobre una base semanal o más frecuentemente, el personal de administración de sistemas debe revisar todas las notificaciones sobre la vulnerabilidad de la seguridad informática emitidas por organizaciones confiables, que afecten los sistemas de la Empresa X.

Comentario: Esta política garantiza que el personal de administración de sistemas, u otro grupo designado, tal como el personal de seguridad informática, está al día en cuanto a seguridad informática. Si este personal conoce

realmente la situación, podría entonces solicitar a la gerencia recursos para actualizar o modificar sus sistemas y, de esta manera, no permanecer vulnerables a los ataques de los hackers o de los espías industriales. La tecnología de sistemas informáticos, particularmente la tecnología Internet, cambia tan rápidamente que se hace imperativo que el personal monitoree regularmente estas notificaciones. Para cuando los proveedores notifiquen a los clientes de una corrección, puede haber transcurrido un largo período de tiempo y, por eso, esta política permite al personal cubrir las fallas que existan en materia de seguridad mucho más rápidamente. La política, de forma deliberada, no especifica cuáles fuentes deben ser consultadas, así como tampoco especifica la tecnología a utilizar para recaudar la información. Algunos fabricantes hoy en día están filtrando estas notificaciones para que los clientes tengan disponible sólo la información que necesitan.

Políticas Relacionadas: ["Planes de Respuesta Ante Emergencias Computacionales,"](#) ["Arreglos de Seguridad,"](#) y ["Explotación de la Vulnerabilidad del Sistema y Datos de la Víctima"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Sistema de Alerta de Seguridad Informática

Política: La gerencia del departamento de Sistemas Informáticos debe establecer, mantener y poner a prueba periódicamente un sistema de comunicaciones que permita a los trabajadores notificar de forma inmediata al personal idóneo los posibles problemas de seguridad informática.

Comentario: Esta política garantiza que la gerencia establecerá y respaldará un sistema de comunicaciones apropiado para la notificación oportuna del personal de seguridad informática. Esto difiere de una estructura organizacional para la pronta movilización del personal de seguridad informática, como por ejemplo, el Equipo de Respuesta ante Emergencias Computacionales. Algunas organizaciones pueden desear extender el alcance de esta política para informar al personal interno sobre la existencia de estos sistemas de comunicaciones y cuándo deben ser utilizados. De no existir dichos sistemas de comunicación, los ataques tienden a ser ignorados, permitiendo que los atacantes continúen utilizando diversos métodos. De no informarse oportunamente la existencia de dichos problemas, existe el riesgo de que las pérdidas sean mayores. Esto se puede evidenciar claramente con las infecciones de virus en

una red informática, donde un retraso de un minuto puede significar mayores interrupciones y mayor pérdida de datos. El proceso de información puede incluir buscapersonas, directorios telefónicos y otros métodos. El designado como responsable del sistema de comunicaciones podría ser el departamento de Seguridad Informática, el de Seguridad Institucional o algún otro grupo, porque es muy importante que la responsabilidad sea designada específicamente.

Políticas Relacionadas: “Equipo de Respuesta Ante Emergencias Computacionales,” “Responsabilidades en el Manejo de Incidentes,” e “Informes de Incidentes”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Problemas por Accesos No Autorizados

Política: Cada vez que se sospeche de accesos no autorizados al sistema o cuando ocurran, el personal de la Empresa X debe tomar medidas de forma inmediata para eliminarlos, o solicitar ayuda al Centro de Atención al Usuario de Sistemas Informáticos Corporativos.

Comentario: Esta política informa al personal técnico y a los usuarios que deben tomar acciones inmediatas para suspender los accesos no autorizados al sistema y que deben buscar inmediata asistencia técnica de expertos a través del Centro de Atención al Usuario, si no pueden detener los ataques por sí mismos. En muchas organizaciones, el Centro de Atención al Usuario se pone en contacto con especialistas técnicos en seguridad informática. En vez de hacerse excesivamente complicada con distintas respuestas a una variedad de problemas, la política simplemente los dirige al Centro de Atención al Usuario. Los procedimientos para manejar la variedad de contingencias pueden ser desarrollados por el personal del Centro de Atención al Usuario conjuntamente con los abogados de la empresa y con los especialistas de seguridad física y de seguridad informática.

Políticas Relacionadas: “Informes de Incidentes”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

10. Mensajes a Atacantes

Política: Un mensaje severo para que desistan debe ser enviado a la fuente de todos los ataques organizados contra los computadores de la Empresa X, siempre que las fuentes y los puntos intermedios de retransmisión puedan ser identificados.

Comentario: La política envía un mensaje a los atacantes en el sentido de que sus actividades han sido descubiertas y que deben detenerlas inmediatamente. En algunas instancias, tal mensaje puede ser suficiente para disuadir al atacante de próximos intentos. Pero si está utilizando un protector, tal como un retransmisor, entonces el mensaje puede ser dirigido al administrador del sitio intermedio. Aun cuando el atacante no reciba el mensaje, algún administrador de ese sitio puede tomar medidas. Esta política también puede estar respaldada por un software nuevo que puede identificar la fuente de los ataques. Esta política se aplica a una amplia variedad de redes, no sólo a Internet. Por ejemplo, podría ser aplicada a conexiones discadas y a una intranet.

Políticas Relacionadas: “Responsabilidad en la Seguridad Informática” y “Problemas en el Sistema de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Resolución de Problemas de Seguridad Informática

Política: Todos los problemas de seguridad informática deben ser manejados con la cooperación del personal de seguridad informática de la empresa o de consultores externos, los equipos de respuesta para la seguridad informática u otros terceros que hayan sido aprobados por el departamento de Seguridad Informática de la Empresa X.

Comentario: Esta política mantiene los problemas de seguridad dentro de la organización, disminuyendo la posibilidad de que entes no autorizados, como los medios de comunicación, se enteren. La política también fomenta el uso del grupo de seguridad informática interno, en lugar de proveedores alternativos de servicios de seguridad informática, lo cual mantiene bajos los costos y garantiza que las políticas internas, las leyes establecidas y los métodos serán aplicados de manera uniforme. Así como los departamentos usuarios finales han tomado sus propias decisiones sobre computadores personales, redes de área local y sistemas cliente-servidor, también en forma creciente lo están haciendo para el área de seguridad

informática. Aunque esta política no requiere que todo el trabajo sea realizado por un grupo de seguridad informática interno, sí exige la aprobación de dicho grupo. La contratación externa es entonces una opción, particularmente cuando no existe suficiente personal interno para manejar ciertos proyectos.

Políticas Relacionadas: “Aprobación de Contratos Externos,” “Responsabilidades de Terceros en la Seguridad Informática,” y “Delegación de la Propiedad de la Información”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

12. Responsabilidades en el Manejo de Incidentes

Política: El personal que tiene la responsabilidad de manejar los incidentes de los sistemas de seguridad informática debe ser designado específicamente y debe recibir la autoridad pertinente para definir los procedimientos adecuados de manejo de incidentes.

Comentario: La gerencia con frecuencia se sorprende cuando ocurre un incidente de seguridad. Es común que la gente no sepa a quién dirigirse o cuáles medidas

deben tomarse. El propósito de esta política es exigir que individuos específicos sean definidos como responsables del manejo de tales incidentes y que todos ellos sepan que son responsables de desarrollar y mantener los procedimientos de manejo de incidentes. La palabra “incidentes”, según el significado aquí otorgado, puede ser interpretada en su más amplio sentido e incluir emergencias y siniestros. Adicionalmente a los planes normales de contingencia, los procedimientos que estos individuos desarrollen pueden incluir las diferentes formas de documentar una investigación, las formas de determinar cómo prevenir la recurrencia de problemas, las formas de reportar un incidente a la gerencia y a terceras personas y las maneras de proteger los registros y las trazas de auditorías, en caso de ser necesarios para administrar disciplina o justicia.

Políticas Relacionadas: “Investigaciones Prolongadas,” “Equipo de Respuesta Ante Emergencias Computacionales,” “Sistema de Alerta de Seguridad Informática,” y “Arreglos de Seguridad”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

8.01.04 Separación de Tareas

1. Rotación de Trabajo

Política: Todos los trabajadores del área de computación que desempeñan importantes puestos de confianza deben ser rotados a puestos diferentes cada 18 meses.

Comentario: Esta política identifica las irregularidades o abusos que pueda cometer un trabajador del área de computación que desempeñe un puesto de confianza. Una segunda intención es adiestrar el personal de forma multidisciplinaria de tal manera de prepararlos para responder en puestos críticos. Después de un cierto lapso de tiempo en ese puesto, son rotados a otro. En algunos casos, mantener el personal en ciertos puestos por un lapso determinado disminuye su posibilidad de identificar y aprovechar las debilidades del sistema de controles internos. No tiene nada de especial el lapso de 18 meses. Podría ser igualmente de 12 meses o cualquier otro lapso de tiempo razonable. La rotación también sirve para ampliar la pericia de los trabajadores,

lo cual se conoce como desarrollo profesional, y para adiestrar futuros gerentes al familiarizarlos con distintos puestos dentro de la organización.

Políticas Relacionadas: “Rotación del Personal Fuera de Sede” y “Pericia en Sistemas”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Separación de Tareas

Política: Cuando un proceso computarizado de la Empresa X involucra información sensible, valiosa o crítica, el sistema debe tener controles que incluyan una separación de tareas u otras medidas compensatorias de control que garanticen que ninguna persona individual tendrá el control exclusivo de este tipo de activos de información.

Comentario: Esta política impide que se cometa fraude, malversación y otros abusos al aprovechar el acceso de un solo individuo a la información de la Empresa X o de

los sistemas que la manejan. Por ejemplo, una empleada bancaria que verifica su propio trabajo y sus reportes, puede extraer dinero ilegalmente sin levantar sospechas. Involucrar a otra persona en un proceso asegura que se llevará a cabo de acuerdo con las instrucciones de la gerencia. Debido a que puede existir sólo un esquema de clasificación de datos, en algunas organizaciones sería aconsejable eliminar las palabras "valiosa o crítica" de esta política. Esta política es importante en aquellas organizaciones donde se utilizan pequeños sistemas distribuidos para el procesamiento de la producción. Esto se debe a que la flexibilidad y la potencia de estos sistemas pequeños permiten reducir el tamaño de la empresa y, a menudo, una sola persona queda para hacer el trabajo de varios ex-empleados.

Políticas Relacionadas:“Separación de Actividades y Datos,’ “Errores y Manipulación de Registros,’ “Instrucciones Sobre la Separación de Tareas,’ “Acceso al Centro de Computación,’ “Trabajo en Areas Restringidas,’ e “Iniciación de Transacciones en Computadores”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

3. Instrucciones Sobre la Separación de Tareas

Política: Si se considera práctico, cada tarea que involucre información sensible, valiosa y crítica requerirá de por lo menos dos personas que coordinen las actividades de manejo de la información, incluyendo la realización de la tarea de principio a fin y la aprobación de los resultados del proyecto.

Comentario:Esta política específicamente define la separación de tareas dentro de una organización. La intención de la misma es suministrar una orientación específica para los especialistas en re-inginería de procesos empresariales, los programadores de mantenimiento y el personal correspondiente. La naturaleza del negocio de cada organización definirá los detalles a ser cubiertos por una política como ésta. Las leyes y los reglamentos específicos de cada industria pueden igualmente señalar los detalles que se mencionen aquí a

futuro. En algunas organizaciones, puede ser apropiado eliminar las palabras "valiosa o crítica", especialmente si no existen políticas relacionadas con estas consideraciones.

Políticas Relacionadas:“Separación de Tareas”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

4. Revisión de Análisis Computarizados

Política: Las decisiones comerciales de la Empresa X superiores a \$1.000.000 y que hayan sido investigadas por un solo individuo, mediante una hoja de cálculo u otra aplicación computarizada, deben ser revisadas en detalle antes de efectuarse acción alguna.

Comentario:Esta política es especialmente pertinente para los computadores personales, las estaciones de trabajo y otros computadores personales, tales como los sistemas cliente-servidor. Lo resaltante de esta política es que requiere la revisión por parte de otra persona del trabajo realizado por un individuo, lo cual puede sacar a relucir errores en la introducción de datos, errores de lógica e información incompleta. Esta política impide que un individuo llegue a una conclusión que luego representará la base de importantes acciones, cuando en realidad la conclusión estaba errada o no suficientemente investigada. La política impone una especie de separación de tareas en el sentido de que las grandes decisiones deben tomarse con la intervención de por lo menos dos personas. Aun cuando la intención original de la política es la de detener los errores, también evita que se cometan fraudes u otros actos intencionales, los cuales pueden ser cometidos si un solo individuo realiza actividades por su cuenta. Lo más importante es que evita que la gerencia tome decisiones erróneas de manera unilateral.

Políticas Relacionadas:“Separación de Tareas,’ “Validación de los Controles,’ y “Validación Cruzada de la Información,’

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

8.01.05 Separación de Tareas de Desarrollo y Operativas

1. Separación de Producción y Desarrollo

Política: El software de aplicaciones comerciales en etapa de desarrollo debe estar estrictamente separado del software de las aplicaciones de producción, a través de sistemas de computación físicamente separados o directorios o librerías separadas por medio de estrictos controles de acceso.

Comentario: La separación entre la producción y el desarrollo de sistemas es uno de los aspectos más importantes de un entorno informático seguro. Si los desarrolladores, usuarios y otros pueden realizar modificaciones al software de producción, entonces, se introduce una amplia variedad de exposiciones a riesgos. Estas exposiciones incluyen los programas caballo de Troya, bombas lógicas y gusanos de redes que podrían ser utilizados para cometer fraudes, estafas y espionaje industrial. Esta política respalda diversos controles de separación de tareas y otorga privilegios de acceso a un reducido número de personas. Algunas organizaciones pueden especificar medios de almacenamiento separados para archivos de producción y de desarrollo. Aunque algunas veces es más difícil de aplicar en ambientes cliente-servidor, redes de área local, computadores personales y sistemas relacionados de menor tamaño, esta política no está restringida a sistemas de gran escala. En la política, las palabras "software de aplicaciones comerciales en etapa de desarrollo" se refieren a tanto al software nuevo como al viejo que se está modificando. La política podría recibir más respaldo si distintos individuos trabajan en las áreas de desarrollo y en las de producción, así como también si se logra la separación física de los equipos de desarrollo y de producción.

Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer," "Separación de Programación y Pruebas," y "Separación de Tareas"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Separación de Tareas en Tecnología Informática

Política: Las siguientes actividades deben ser realizadas por distintas personas: el desarrollo y mantenimiento del código fuente de las aplicaciones de producción, el período de prueba y operación de las aplicaciones de producción y el manejo de los datos de las aplicaciones de producción.

Comentario: La política gira instrucciones a la baja gerencia en el sentido de establecer una separación apropiada de tareas alrededor de las aplicaciones de operaciones de producción. La primera de las tres categorías mencionadas tiene que ver con las tareas del programador, la segunda con las tareas del operador del computador y la tercera con las tareas del usuario. Debido a que distintas habilidades están relacionadas con estas tres áreas, será difícil que una persona que trabaje en un área sepa qué hacer en otras. La documentación para cada uno de estos tres grupos debe ser almacenada por separado para reforzar esta dificultad. El término "período de prueba" se refiere a los pasos por los que debe pasar un programa de aplicaciones previo a ser utilizado en un ambiente de producción. Estos pasos incluyen realizar pruebas a las aplicaciones, obtener la aprobación del Propietario que las patrocina, pasar a la operación de producción y suministrar los trabajos. El proceso de "manejo de los datos", tal como está aquí descrito, incluye la carga de nuevos datos, y la modificación y eliminación de los datos que están ya cargados en el computador. La organización que adopte esta política podría disfrutar de menores probabilidades de sufrir fraude, de una creciente confiabilidad de sus sistemas y de menores probabilidades de errores u omisiones.

Políticas Relacionadas: "Privilegios del Personal Técnico" y "Documentación de los Controles de Cambios"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

3. Separación de Programación y Pruebas

Política: El software de aplicaciones de producción en etapa de desarrollo debe permanecer estrictamente separado de este mismo tipo de software en período de prueba, a través de sistemas informáticos físicamente separados o directorios o bibliotecas separadas con estrictos controles de acceso.

Comentario: La intención de esta política es proporcionar seguridad en la separación de los ambientes de producción y desarrollo, así como la de impedir la modificación no autorizada de software después de ejecutarse las pruebas, lo cual conlleva a que el software se ubique en un entorno de producción y luego se utilice para cometer fraude, estafa, sabotaje o espionaje industrial. La política podría ser respaldada más amplia-

mente si se tienen individuos trabajando por separado en el área de desarrollo y de pruebas, así como también al separar físicamente al equipo de desarrollo del de producción.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#)” y “[Separación de Producción y Desarrollo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Prueba del Software

Política: Los trabajadores que han estado involucrados en el desarrollo de software para aplicaciones empresariales específicas, no deben estar involucrados en las pruebas formales o en las operaciones cotidianas de producción de dicho software.

Comentario: Los desarrolladores deben probar sus programas a medida que los desarrollan. Esta política no se refiere a las pruebas informales que se llevan a cabo durante el trabajo de programación y desarrollo de los programas. Si se utilizan las palabras “prueba formal”, esta política se refiere al proceso a través del cual la

gerencia usuaria y la gerencia de sistemas se sienten satisfechas porque el sistema se desempeña de acuerdo con las especificaciones. Si un programador u otro desarrollador tuviera que realizar una prueba formal de su propio trabajo, se sentiría tentado a escoger sólo aquellas pruebas que demuestren que ciertas medidas de control funcionan bien e ignorar aquellas potencialmente problemáticas. Aun cuando no tengan la intención de parecer ociosos, los desarrolladores pueden no considerar todas las circunstancias reales a las que se someterá el software. Se necesita otra revisión para validar que la aplicación funcionará adecuadamente. Aunque resulta más difícil de lograr en el ambiente cliente-servidor, en las redes de área local, en los computadores personales y en ambientes parecidos de sistemas a menor escala, esta política no está restringida a sistemas de gran escala. Esta política es una manifestación del principio de separación de tareas.

Políticas Relacionadas: “[Separación de Tareas](#)” y “[Acceso del Desarrollador a la Información de Producción](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8.01.06 Gestión Externa de Instalaciones

1. Riesgos y Expectativas de Contratistas

Política: Cuando se utiliza un contratista externo para que administre instalaciones de procesamiento informático, se deben identificar por adelantado los riesgos en que se pueda incurrir, establecer controles para disminuir estos riesgos e incorporar al contrato todas las expectativas del contratista.

Comentario: Esta política garantiza que se tomarán medidas apropiadas y eficaces para asegurar que las instalaciones de la Empresa X están adecuadamente controladas y protegidas cuando la responsabilidad de la administración de las instalaciones recae sobre un tercero. Las organizaciones están contratando externamente diversos aspectos de sus negocios, inclusive la gerencia de sus instalaciones. Sin una idea clara de los

riesgos, de los controles y de las expectativas del proveedor externo de este servicio, la Empresa X podía estar expuesta a varias amenazas, tales como el robo de servicios y el fraude. Es imperativo que cualquier arreglo de este tipo de servicio se examine y revise cuidadosamente antes de firmarse un convenio final.

Políticas Relacionadas: “[Aprobación de Contratos Externos](#),” “[Ubicación del Centro de Computación y Comunicaciones](#),” “[Infraestructura de Respaldo para Centro de Datos](#),” y “[Planes de Recuperación Ante Desastre Computacional](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8.02 Planificación y Aceptación del Sistema

8.02.01 Planificación de la Capacidad

1. Implantación de Sistemas Multiusuario

Política: Los trabajadores no deben instalar servidores para la intranet, ni foros electrónicos, ni redes de área local, ni conexiones con módems a redes internas ya existentes, ni otros servicios multiusuario para transmitir información sin la autorización específica del director del departamento de Seguridad Informática.

Comentario: Esta política asegura que los usuarios no se encuentran instalando sistemas de comunicaciones que puedan comprometer inadvertidamente la información y los sistemas de una organización. Esta política es particularmente importante para el ambiente de computadores personales y de estaciones de trabajo y sistemas cliente-servidor, donde los usuarios frecuentemente ignoran los parámetros internos o las instrucciones emitidas por el departamento de Sistemas Informáticos. De no existir un proceso de autorización centralizado, respaldado por un proceso de auditoría de obligatorio cumplimiento, es posible que algunos usuarios generen vulnerabilidades importantes en la seguridad informática sin que los departamentos de Seguridad Informática, el departamento de Telecomunicaciones o el departamento de Sistemas Informáticos tengan conocimiento de ello. La responsabilidad de otorgar autorizaciones puede ser fácilmente transferida a otro gerente de alto nivel y no permanecer en las manos del director del departamento de Seguridad Informática. El énfasis de esta política en los sistemas multiusuario es el reflejo de que poseen mayor información que los sistemas monousuario, y como tal representan riesgos mayores.

Políticas Relacionadas: “[Cambios en la Línea de Comunicación](#),” “[Aislamiento de Sistemas con Información Secreta](#),” y “[Autorización para Servidor Intranet](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

2. Interconexión de Sistemas

Política: No deben establecerse conexiones en tiempo real entre dos o más sistemas informáticos internos a no ser que el departamento de Seguridad Informática determine que dichas conexiones no pondrán en peligro la seguridad informática.

Comentario: Esta política mantiene determinada información dentro de ciertas áreas de la organización y de esta forma controla su diseminación. Este objetivo implica el aislamiento para lograr la seguridad. Por ejemplo, la información salarial de los empleados podría estar guardada sólo en los computadores del departamento de Recursos Humanos. El establecimiento de una conexión con la red local interna puede abrir un camino para la diseminación no autorizada de esta información privada. Esta política no excluye el traslado de cintas, discos, CD-ROM y otros medios de almacenamiento entre sistemas. Generalmente el traslado en tiempo real de los datos es más fácil de controlar. Una conexión en tiempo real con frecuencia permite que personas no autorizadas tengan rápido acceso a la información dejando poca o ninguna huella para auditorías posteriores. Se recomienda una modificación de esta política para ampliar su alcance hasta cualquier conexión con un sistema interno.

Políticas Relacionadas: “[Cambios en la Línea de Comunicación](#),” “[Aislamiento de Sistemas con Información Secreta](#),” y “[Autorización para Servidor Intranet](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

8.02.02 Aceptación del Sistema

1. Configuración del Sistema

Política: Todos los servidores de la Empresa X, los servidores, los cortafuegos, y otros computadores multiusuario, deben estar configurados de conformidad con los requisitos de seguridad publicados por el departamento de Seguridad Informática.

Comentario: Esta política impide que los administradores de sistemas, los operadores de computadores u otros miembros técnicos del personal, configuren los computadores multiusuario en forma insegura. Puede que los miembros del personal técnico tengan otras ideas en cuanto a la configuración de un sistema, y esta inconsistencia puede llevar a intrusiones innecesarias, a

fallas catastróficas y a la necesidad de servicio técnico. La consistencia es esencial si la organización quiere lograr un nivel razonable de seguridad informática. Esta política logra consistencia al especificar que estos miembros del personal técnico deben trabajar de conformidad con los requisitos de Seguridad Informática. Dicha política no constituye una guía de acuerdo a la cual estos sistemas deben estar configurados. En lugar de eso, especifica que la guía existe y que los sistemas multiusuario deben utilizarla. Muchas organizaciones no querrán que dicha guía esté plasmada en la forma de una política ya que cambiará muy rápidamente.

Políticas Relacionadas: “[Plantillas para Configuración de Sistemas](#)” y “[Configuración de Cortafuegos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Documentación para Sistemas de Producción

Política: Cada usuario que desarrolle o ponga en práctica cualquier software o hardware que vaya a utilizar la Empresa X en sus actividades comerciales de producción, deben documentar el sistema en forma clara antes de su entrada en producción.

Comentario: Si el tipo de documentación descrita en esta política no está disponible ni vigente, la indisponibilidad repentina de una persona clave puede significar que el procesamiento de los datos de producción que supervisan finalizará de manera abrupta. Esta política es particularmente importante en sistemas pequeños, tales como los de los computadores personales, las estaciones de trabajo, las redes de área local, los sistemas cliente-servidor, y los sistemas departamentales. La programación por parte de los usuarios finales de sistemas comerciales de producción puede acarrear pérdidas cuantiosas si no está disponible la documentación correcta. Esto podría pasar, por ejemplo, si la persona que desarrolló el sistema abandona la organización y nadie más sabe manejar dicho sistema. También es probable que dicha documentación sea crítica para los planes de contingencia. También podrían incluirse en la política palabras que abarquen la necesidad de actualizar la documentación periódicamente, o cada vez que se lleven a cabo cambios mayores.

Políticas Relacionadas: “[Documentación de las Aplicaciones de Producción](#)” y “[Documentación de Adiestramiento y Operaciones](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Evaluación de Nuevas Tecnologías

Política: Toda tecnología nueva debe ser evaluada y aprobada por la gerencia de Seguridad Informática, antes de ser utilizada con el software de aplicaciones de producción, con el hardware o en la red de la Empresa X.

Comentario: Esta política garantiza que el departamento usuario o Sistemas Informáticos no instalará tecnología nueva sin primero tomarse el tiempo para evaluar las consecuencias que esto podría tener en materia de seguridad. Debido a que tanto la gerencia del departamento usuario como la gerencia del departamento de Sistemas Informáticos quieren poner rápidamente en marcha la nueva tecnología, ellos preferirían omitir la revisión de la seguridad. Esta política especifica que una revisión de seguridad debe ser parte de un proceso de control de cambios si se trata de nueva tecnología, lo cual justifica que se le tenga una consideración especial ya que los problemas de seguridad potenciales no se pueden apreciar sino después de cierto tiempo. Esta política refleja la importancia que cada día va adquiriendo el rol de consultor técnico desempeñado por el departamento de Seguridad Informática. Ejemplos de la nueva tecnología a la cual la política hace referencia incluyen los asistentes digitales personales, las redes privadas virtuales y las redes inalámbricas.

Políticas Relacionadas: “[Migración de Software](#)” y “[Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Controles de Sistemas de Producción

Política: Los sistemas de aplicación nuevos o que hayan experimentado grandes modificaciones deben haber sido autorizados por escrito por el gerente del departamento de Seguridad Informática antes de ser utilizados para el procesamiento de la producción.

Comentario: Esta política requiere que el departamento de Seguridad Informática revise los esfuerzos internos que se han realizado en el desarrollo de sistemas, para garantizar que se han establecido los controles necesarios. Esta política impide que sean puestas en producción las aplicaciones que no tengan el debido control. En vez de hacer referencia al departamento de

Seguridad Informática, la política podría hacer referencia al departamento de Auditoría de Tecnología Informática. De manera indirecta, esta política motiva el uso de equipos para el desarrollo de sistemas con personal adiestrado en materia de seguridad, aunque algunas organizaciones piensen que esta política le da mucho poder al departamento de Seguridad Informática. Se recomienda la distribución de esta política tanto a los usuarios finales como a la gerencia para sugerirles no modificar los sistemas de producción sin pasar por los canales ordinarios. Algunas organizaciones incluso llegan al extremo de solicitar a la gerencia del departamento usuario que reconozca y apruebe, mediante la firma, la existencia de los controles que se aplican a los sistemas. Este proceso ayuda a los gerentes de los departamentos usuarios a aprender a ver la seguridad con mayor seriedad.

Políticas Relacionadas: "Proceso de Control de Cambios para Aplicaciones de Negocios," "Desarrollo de Sistemas por Usuarios Finales," y "Proyectos que Involucran Seguridad Humana"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Aceptación de Aplicaciones de Producción

Política: Deben obtenerse las firmas de Operaciones Informáticas, del departamento usuario correspondiente y de Auditoría de Tecnología Informática, en señal de aceptación y aprobación, antes de que los programas entren en producción en un computador multiusuario.

Comentario: Esta política garantiza que en las máquinas multiusuario se ejecutarán sólo aquellas aplicaciones que han sido debidamente autorizadas por los representantes gerenciales correspondientes. El departamento de Seguridad Informática podría ser añadido a la política. La referencia a "Auditoría de Tecnología Informática" podría ser reemplazada por la referencia a "Seguridad Informática", dependiendo de lo que se haya establecido en la misión de los grupos dentro de la organización. Los servidores de redes de área local, los servidores de correo, los servidores en redes cliente-servidor, y otras máquinas de sistemas de menor escala, están definitivamente dentro del alcance de esta política. Esta política tiene que ver con autorizaciones emitidas por diferentes grupos, los cuales tienen objetivos adicionales a la inclusión de controles. Esta política hace énfasis en los sistemas multiusuario porque merecen especial atención, ya que usualmente están conectados en red y contienen la mayor cantidad de información valiosa, sensible y crítica. La política

podría ser modificada para incluir las grandes modificaciones experimentadas a través del proceso de mantenimiento de los programas.

Políticas Relacionadas: "Controles de Sistemas de Producción" e "Implantación de Sistemas Multiusuario"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Desarrollo de Sistemas por Usuarios Finales

Política: Todo software desarrollado por usuarios finales que maneje información sensible, crítica o valiosa, debe recibir la aprobación del departamento de Seguridad Informática antes de su utilización en el procesamiento de la producción.

Comentario: Provocan inquietud los esfuerzos de desarrollo de software por parte de los usuarios finales, ya que éstos implantan ambientes de procesamiento de producción en sus propias oficinas sin involucrar al departamento de Sistemas Informáticos ni a Seguridad Informática. Esto deviene a menudo en la falta de controles necesarios en los sistemas cliente-servidor, las redes de área local y los computadores personales que manejan actividades empresariales de importancia. Esta política define el proceso que garantiza la integración de dichos controles a estos sistemas. En muchas organizaciones se necesitarán políticas separadas, una para los usuarios finales y una para los técnicos, en lo relativo al proceso de control de cambios. Más allá de lo descrito en esta política, sería aconsejable obtener autorización adicional por parte del departamento de Sistemas Informáticos para garantizar que se toman en debida cuenta las normativas aplicables a las redes corporativas, la documentación y otros asuntos. Las palabras "Departamento de Seguridad Informática" utilizadas en esta política podrían ser reemplazadas por "Departamento de Auditoría de Tecnología Informática".

Políticas Relacionadas: "Controles de Sistemas de Producción"

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

7. Planes de Contingencia en Conversión de Software

Política: Cada vez que la puesta en práctica de un software de producción nuevo o con modificaciones significativas genere problemas a la Empresa X, con

posibles pérdidas superiores a \$1.000.000, la gerencia debe preparar un plan de contingencia relacionado con la conversión, para que refleje las diversas vías que garanticen la continuidad del servicio a los usuarios finales potencialmente afectados.

Comentario: Esta política garantiza que la gerencia ha definido procedimientos específicos para manejar los problemas relacionados con conversiones mayores. No hay nada de especial con respecto a la cifra utilizada en esta política, por cuanto el monto a utilizar simplemente debería reflejar las necesidades de la organización. El uso de una cifra tope es útil desde el punto de vista de seguridad, ya que logra que la gerencia realice una evaluación de riesgo, planteándose si puede realmente perder \$1.000.000 o más en el proceso de conversión. Algunas personas querrán especificar lo que representa una pérdida de este tipo; es decir, por ejemplo, los ingresos perdidos, los esfuerzos adicionales en relaciones públicas, la consultoría adicional y el uso adicional de servicio informático o de oficina. Debido a que no sólo está dirigida a los aspectos de software de la conversión, esta política implícitamente tiene que ver con el hardware, el trabajo en red, las relaciones con el cliente y otros factores.

Políticas Relacionadas: “[Procedimientos de Retorno](#)” y “[Enunciados Sobre el Impacto de la Seguridad](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Análisis del Impacto sobre la Seguridad Informática

Política: Cada vez que se vaya a cargar información sensible en los computadores, o a utilizarse de maneras sustancialmente nuevas y diferentes, se debe llevar a cabo una evaluación de riesgo de los impactos potenciales sobre la seguridad.

Comentario: Al estar conscientes de que la seguridad puede ser fácilmente suprimida en muchos sistemas, algunas organizaciones prohíben la carga de datos sensibles en cualquiera de sus computadores. Por ejemplo, un banco grande nunca colocaría la evaluación de desempeño de su personal administrativo en ningún computador o red. Estos datos serían guardados en discos flexibles y mantenidos bajo llave de no estar en uso. Aunque este enfoque resulta demasiado cauteloso para la mayoría de las organizaciones, la preocupación subyacente es válida. Algunas organizaciones pudieran limitar la política a computadores conectados en red. La política podría ser redefinida para que hiciera referencia

a modificaciones mayores en los sistemas y para que involucre información sensible. De manera similar y para ampliar su alcance, la política podría ser modificada para hacer referencia a información "sensible, valiosa, y crítica" en vez de sólo a información "sensible". Se recomienda esta modificación, a pesar de que incrementa sustancialmente el costo de la puesta en práctica de la política. Aquí se asume que la organización ha adoptado previamente una política de clasificación de datos donde se define la palabra "sensible".

Políticas Relacionadas: “[Especificaciones para Software Desarrollado Internamente](#)” y “[Enunciados Sobre el Impacto de la Seguridad](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9. Enunciados Sobre el Impacto de la Seguridad

Política: Antes de ponerse en producción, cada sistema de aplicación comercial nuevo o con modificaciones significativas debe incluir una breve declaración del impacto sobre la seguridad, redactada de acuerdo con los procedimientos establecidos.

Comentario: La declaración del impacto sobre la seguridad debe explicar cómo cambiaría la seguridad del sistema de apoyo al poner en funcionamiento el sistema nuevo o modificado. Esta política se refiere a los cambios en las aplicaciones comerciales en vez de los cambios en la forma que es manejada cierta información. Esta política también puede ser ampliada con el fin de incluir un bosquejo de los componentes de una declaración del impacto sobre la seguridad, por ejemplo, las normas éticas y los riesgos a considerar. Esta política también se puede modificar para definir cuándo, dentro del ciclo de vida del desarrollo de los sistemas, debe redactarse una declaración de efecto, la cual resulta más eficaz si se implanta al inicio del proceso. El alcance de esta política puede, en forma adicional, ser ampliado con el propósito de requerir que la declaración del efecto sobre la seguridad sea revisada por la gerencia de Auditoría de Tecnología Informática o la gerencia de Seguridad Informática.

Políticas Relacionadas: “[Análisis del Impacto sobre la Seguridad Informática](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Revisión del Impacto Sobre la Privacidad

Política: Todo proyecto de desarrollo de sistemas de envergadura, o proyecto de mejoramiento, que pueda afectar la privacidad de las personas, debe ser revisado de antemano por un comité independiente, el cual debe determinar si los individuos estarán bajo riesgo o en desventaja como resultado del proyecto y recomendar o bien las medidas correctivas o bien la cancelación del proyecto, de ser necesario.

Comentario: Esta política requiere que los desarrolladores de sistemas tomen en cuenta las consecuencias que sobre la privacidad tienen los nuevos sistemas que desarrollen. Un comité de privacidad podría estar conformado por personas pertenecientes a la organización o por personas externas e internas. Algunas organizaciones pueden especificar el número de miembros del comité y su conformación. Dicho comité sólo está justificado en aquellas industrias, tales como las de servicios financieros y las de la salud, donde la privacidad es de gran importancia. Lo provisto por esta política no confiere derechos al comité para cancelar el proyecto, posponerlo o usurpar las prerrogativas de la gerencia. De todas maneras, la existencia de un informe elaborado por el comité debe alertar a la gerencia en el sentido de tomar ciertas medidas. Si la gerencia no las toma, estaría obviando su deber fiduciario de proteger los activos de la organización.

Políticas Relacionadas: “Comité de Gestión de Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Aceptación del Usuario de las Medidas de Seguridad Informática

Política: Todos los controles de seguridad informática deben ser aceptados y respaldados por las personas que utilizan y son supervisados por dichos controles.

Comentario: La aceptación de las medidas por parte de los usuarios es esencial para el éxito de todos los controles. Estos individuos deberían estar involucrados en el proceso de toma de decisiones relativas a los controles. Por ejemplo, los representantes de los sindicatos podrían estar involucrados en las conversaciones acerca del uso de los sistemas informáticos para monitorear el trabajo de los empleados. Esta política explícitamente exige a la gerencia explicar y justificar los controles a sus empleados. Dichas comunicaciones refuerzan la motivación de los empleados a cumplir las medidas de seguridad. Si los empleados entienden las

razones de la existencia de las medidas de seguridad, podrían lograr los mismos objetivos aún cuando dichas medidas de seguridad fallen. La política podría ser modificada para incorporar alguna indicación de para cuándo deberían obtenerse la aceptación y el respaldo.

Políticas Relacionadas: “Controles Mínimos en Sistemas Informáticos” y “Controles de Acceso al Sistema de Computación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Plantillas para Configuración de Sistemas

Política: Todo computador en la Empresa X de uso general, debe ser configurado y personalizado en concordancia con una de las tres plantillas de seguridad emitidas por el departamento de Seguridad Informática.

Comentario: La intención de esta política es la de establecer la existencia de un esquema de clasificación informática de tres niveles, y exigir que todos los computadores de uso general estén personalizados y configurados en concordancia con los requerimientos de clasificación. Este esquema reconoce el hecho de que cada uno de los tres tipos de computadores tiene diferentes requerimientos de seguridad. Por ejemplo, un sistema de escritorio tendrá un registro mínimo o no existente mientras que un servidor de infraestructura, tal como un servidor de correo, tendrá un registro muy activo. Un servidor límite, por otro lado, tal como un cortafuego, tendrá el máximo registro disponible. Estas clasificaciones requieren de seguridad sólo donde se le necesite y, por lo tanto, reducen el costo total. La existencia de un esquema de tres niveles re establece el control centralizado sobre la configuración y personalización de los computadores. En muchas organizaciones, los usuarios finales han asumido las operaciones de los computadores locales y utilizan una amplia variedad de enfoques en cuanto a configuración y personalización aun dentro de la misma organización. Al normalizar estas clasificaciones informáticas, la organización puede ayudar a restaurar el orden y la seguridad operativa a lo largo de todos los departamentos. El uso de plantillas facilita la adición de servicios centralizados de seguridad informática, tales como un sistema de administración de redes o un sistema centralizado de detección de intrusos. Un ejemplo de una decisión relativa a la configuración lo representa la especificación del número mínimo de caracteres que deben tener las contraseñas. Un ejemplo de una decisión relativa a la personalización lo representa la especificación del paquete del software

antivirus que debe ser instalado y ejecutado en todas las máquinas definidas dentro de un tipo de plantilla. Un computador no puede integrar más de una de estas tres categorías.

Políticas Relacionadas: “Guía de Estilo de Intranet,” “Configuración de Seguridad,” y “Controles de Acceso al Sistema de Computación”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

8.03 Protección Contra Software Malicioso

8.03.01 Controles Contra Software Malicioso

1. Acceso de Sistemas a la Red

Política: Los sistemas que no poseen los parches de software adecuados o que estén contaminados con virus, deben ser desconectados de la red de la Empresa X.

Comentario: Esta política reconoce el hecho de que un sistema en una red contaminado con virus pone en significativo riesgo a los otros sistemas de la misma red. La intención de esta política es informar a los usuarios que estarán temporalmente desconectados de la red, y todo lo relativo a dicha conexión, si no colocan rápidamente parches y no cargan la última versión del software antivirus. La política proporciona un mecanismo de exigencia a los usuarios para que éstos presten atención a la seguridad, que en condiciones normales ha sido ignorada, pensándose que es responsabilidad de los técnicos informáticos. La política puede ser puesta en práctica a través de un software para identificación de vulnerabilidades que permite evaluar el software instalado en computadores remotos, y un software detector de virus, instalado en un servidor de correo o en un cortafuego. Toda vez que el acceso a la red es denegado al usuario, estos mecanismos de evaluación de software pueden ser ejecutados nuevamente para determinar si el usuario ha tomado las acciones necesarias. Es necesario habilitar una conexión con las máquinas de usuarios remotos para que se puedan ejecutar estos mecanismos de evaluación. Aunque esta política ha sido redactada para una red interna, podría fácilmente ser modificada para aplicarse en una organización que ofrezca sus servicios en la Internet, en cuyo caso la palabra "usuarios" se convertiría en "clientes".

Políticas Relacionadas: “Conexiones a Internet” y “Autorización para Conexiones a Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Erradicación de Virus de Computadores

Política: Cualquier usuario que intuya la existencia de un virus debe apagar inmediatamente el computador correspondiente, desconectarlo de todas las redes, llamar al Centro de Atención al Usuario y no intentar eliminar el virus.

Comentario: Esta política evita que los usuarios intenten eliminar los virus de sus sistemas. Si los usuarios eliminan los virus por su cuenta, sus esfuerzos podrían resultar en la propagación del virus o en la destrucción de datos o programas. Por ejemplo, los usuarios pueden intentar comprobar el funcionamiento de un programa residente en un disco flexible en el computador de un compañero de trabajo y, sin querer, propagar el virus. En vez de hacer esto, y para solventar el problema, se debe solicitar el apoyo de los expertos del Centro de Atención al Usuario o el de una consultora externa. Algunas organizaciones podrían ampliar el alcance de la política y sugerir a los usuarios abstenerse de usar discos flexibles u otros medios de almacenamiento que hayan sido utilizados en un computador infectado.

Políticas Relacionadas: “Informe de Sospecha de Virus”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Erradicación de Virus por Administradores del Sistema

Política: Los usuarios no deben intentar eliminar los virus de sus sistemas, a menos que lo hagan mientras estén en comunicación con un Administrador de Sistemas.

Comentario: Esta política evita que los usuarios propaguen, sin querer, el virus en su afán de aislar y entender el problema. La política asume que se cuenta con un sistema de detección de virus en los sistemas internos de menor escala susceptibles a virus, y que los usuarios serán alertados sobre una posible contaminación por virus. La política exige a los usuarios solicitar asistencia técnica inmediata, en vez de realizar por sí mismos estas complejas tareas. Este enfoque implica que sólo los administradores de sistemas necesitan ser adiestrados en las pericias del uso de herramientas para la eliminación de virus, mas no el público usuario en general. Este enfoque garantiza, igualmente, que se elaborarán informes acerca de la contaminación por virus con la finalidad de llevar las estadísticas correspondientes. Otro aspecto importante de este enfoque es la habilitación del software de registro asociado con algunos paquetes de detección de virus, donde dichos registros indican las acciones que fueron tomadas para la eliminación del virus y a menudo representan referencias esenciales para la restauración del entorno informático presente antes de la contaminación. Estos registros pueden capturar al virus mismo, de tal manera que el proveedor del software antivirus lo pueda actualizar simultáneamente y pueda detectar virus nuevos y versiones mutantes de virus anteriores.

Políticas Relacionadas: “[Erradicación de Virus de Computadores](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Descarga de Software

Política: Los trabajadores no deben descargar software de ningún sistema externo a la Empresa X.

Comentario: Esta política reduce notablemente las posibilidades de infección por virus, gusanos y otros virus ocultos. El software externo no autorizado puede además causar incompatibilidad, escasez de espacio en

disco y reducción de la productividad de los trabajadores. Esta política no prohíbe la descarga de datos desde sistemas de terceros, pero sí prohíbe la descarga de su software. Algunas organizaciones querrán añadir palabras para aclarar esta distinción, lo cual se debe a que los virus, en la mayoría de los casos, se adhieren al software y no a los datos, aunque un virus de macro sí se adhiere a datos, tales como los de los archivos de hojas de cálculo. La única forma segura de evitar estos nuevos virus es el de simplemente descargar textos ASCII, datos RTF o prohibir los anexos en los correos electrónicos. La política, tal como está redactada aquí, motiva el uso de normas para seleccionar paquetes de software, en vez de permitir que los usuarios utilicen libremente el software de su preferencia. Esto genera un entorno informático más amigable de controlar y de gestionar. Aquellas organizaciones que tienen una gran inquietud en lo que concierne al tema de los virus, podrían adoptar una política tan estricta como ésta, aunque podría surtir el mismo efecto exigir que todo el software de terceros sea examinado con paquetes antivirus antes de su uso. Otra opción sería requerir el permiso de un coordinador local de seguridad informática antes de descargar el software. Igualmente podría utilizarse software para la gestión de licencias de software para evitar el uso de software externo que aún no haya sido aprobado por la gerencia. Algunos cortafuegos pueden ser utilizados para reforzar esta política. Debido a que los virus y los códigos maliciosos sólo han constituido un problema en sistemas pequeños, esta política puede ser aplicada principalmente a las estaciones de trabajo, los computadores personales, las redes de área local y los sistemas cliente-servidor. Esta política adquiere cada vez mayor importancia en aquellas organizaciones conectadas a la Internet.

Políticas Relacionadas: “[Exploración del Software](#),” “[Operadores de Entrada de Datos](#),” y “[Descarga de Software Desde Un Sitio Espejo en Internet](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

5. Exploración del Software

Política: Los trabajadores no deben utilizar software que haya sido suministrado por fuentes externas a la empresa o que provenga de personas u organizaciones distintas de los proveedores conocidos y confiables; pero sí podrían utilizar software que haya sido verificado o autorizado por el departamento de Seguridad Informática o por el coordinador local de seguridad informática.

Comentario: Esta política reduce notablemente las posibilidades de contaminación por virus, gusanos, caballos de Troya u otros programas no autorizados. La aplicación de esta política no está restringida a los sistemas de producción. Estos programas no autorizados se propagan rápidamente y no establecen distinción entre sistemas de producción y sistemas no relacionados con producción. La política sólo requiere un mínimo trabajo adicional para el manejo del software proveniente de fuentes externas. Normalmente, los usuarios utilizan software que ha sido aprobado para uso interno y con la respectiva licencia de los proveedores. Esta política limita las rutinas de software que pueden ser ejecutadas por los usuarios. La política también desalienta el copiado no autorizado de software para el cual la Empresa X no tiene licencia de uso. Aunque no tiene que estar explícito en la política, las pruebas realizadas al software deben llevarse a cabo en máquinas aisladas de la red. Algunas organizaciones querrán especificar exactamente qué significa proveedor conocido y confiable. Otras organizaciones querrán ampliar el alcance de la política con el fin de que se documenten las pruebas realizadas al software proveniente de fuentes externas. Algunas organizaciones podrían solicitar modificaciones en la política de tal manera que se hagan pruebas a todas las copias de software que provengan de fuentes no confiables y no sólo a una copia. Esta política no impide a los usuarios descargar software que provenga de terceros, pero sí el ejecutarlo hasta que no haya sido examinado. Su cumplimiento puede迫使 mediante el uso de software de gestión de licencias o software para controlar modificaciones en computadores personales.

Políticas Relacionadas: ‘[Descarga de Software](#),’ ‘[Carga de Programas Externos](#),’ ‘[Información Descargada](#),’ ‘[Revisión de los Convenios de Licencia del Software](#),’ e ‘[Informe de Sospecha de Virus](#)’

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

6. Sistema de Prueba Antivirus

Política: Cada vez que se reciba software o archivos desde entes externos, deben ser analizados en una máquina independiente de la red antes de ser utilizados en los sistemas informáticos de la Empresa X.

Comentario: Esta política mantiene límites estrictos alrededor de la red de la organización y de los sistemas informáticos internos. Esta política establece que el software suministrado por los proveedores, los archivos suministrados por los socios de organizaciones profesionales y todo aquel material que provenga de entes externos, deben ser analizados antes de ser utilizados en los sistemas informáticos de la Empresa X. Los virus pueden estar incrustados en hojas de cálculo además de estarlo, como hasta ahora, en programas. Esta política puede ser percibida como muy estricta, muy costosa o inconveniente para algunas organizaciones, por el hecho de tener que mantener una máquina independiente para los análisis del material suministrado por entes externos. El análisis que se le hace a todo material proveniente de entes externos mediante programas que son invocados cada vez que un disquete es introducido en una unidad de disquete hace aparentemente innecesario la existencia de una máquina no relacionada al sistema de producción. Del mismo modo, algunos cortafuegos pueden verificar archivos de datos, correos electrónicos y ejecutables. Un beneficio de esta política es que se pueden guardar en la máquina independiente los registros de los análisis realizados. Este registro puede suministrar información esencial para el rastreo y la erradicación del virus. La necesidad de utilizar una máquina independiente disuade a los usuarios de utilizar software distinto al establecido, bajo licencia y previamente analizado, lo que garantiza que éste será el que la organización utilizará en forma constante. Esta política será reemplazada por software de gestión de licencias de computadores personales. La definición de producción que establece la Empresa X es crítica para esta política. Si los computadores personales no son considerados máquinas productivas, la política será fácilmente puesta en práctica a través de programas de verificación residentes. Si los computadores personales están conectados a una intranet, entonces se requerirá de una máquina independiente o de un proceso de desconexión de la intranet.

Políticas Relacionadas: ‘[Información Descargada](#)’

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Software y Ejecutables Salientes

Política: Todos los archivos contentivos de declaraciones de software o de ejecutables deben tener una certificación que establezca que están libres de virus antes de ser enviados a terceros.

Comentario: Esta política garantiza que los archivos de software y de ejecutables que distribuye la Empresa X a terceros, no propagan virus. La política se refiere a las transmisiones salientes de archivos, que a menudo no son restringidas, mientras que las transmisiones entrantes de archivos son frecuentemente monitoreadas de cerca. La política asume que cada usuario posee la utilidad de verificación de virus más novedosa en su computador, y que cuenta con las pericias necesarias para manejar dicha utilidad. Dicha verificación de virus no es requisito esencial para los archivos salientes que tengan formato de texto, o un formato enriquecido de texto, debido a que ninguna declaración de ejecutables se encuentra incluida en tales archivos. La política se abstiene en forma deliberada de hablar sobre una vía para la transmisión, ya que la misma es aplicable a cualquier tipo de transmisión.

Políticas Relacionadas: “[Descarga de Software](#)” y “[Exploración de Software Descargado](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

8. Instalación de Software Antivirus

Política: Debe estar instalado y habilitado software para verificar la presencia de virus en todos los cortafuegos de la Empresa X, los servidores FTP, los servidores de correo, los servidores de la intranet y las máquinas de escritorio.

Comentario: Esta política requiere que el software para el filtrado de virus sea residente y esté habilitado para su uso en diferentes localidades de la red interna. La política no establece las veces en que debe llevarse a cabo un rastreo o verificación. Dado que algunos archivos pueden ser cifrados o descifrados en cualquiera de estos tres puntos, un paquete para rastreo de virus utilizado en una localidad puede dejar pasar un virus que haya sido parte de la transmisión. Lo mismo pudiera decirse de las técnicas de compresión de datos, aunque muchos paquetes de rastreo de virus se pueden adecuar a la compresión de datos. Debido a que los virus podrían ser transmitidos en cualquiera de estas tres localidades, y dado que mientras más rápido se detecten y eliminén menos se propagarán, se recomienda un chequeo de virus en todas las localidades especificadas.

Políticas Relacionadas: “[Múltiples Paquetes Antivirus](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Múltiples Paquetes Antivirus

Política: Se deben utilizar por lo menos dos paquetes de software para rastreo de virus en cada una de las ubicaciones de la red de la Empresa X en las cuales ingresan correos electrónicos y otros archivos.

Comentario: Cada vez se hace más difícil detectar todos los tipos de virus a través de los paquetes de software para rastreo, aun cuando se apliquen rápidamente y en sus versiones más actualizadas. Para reducir el nivel de riesgo, algunas organizaciones procesan varios de estos sistemas de rastreo de virus en servidores de correo, cortafuegos y otras máquinas que aceptan archivos entrantes, inclusive correos electrónicos. Esta política podría tener un impacto negativo sobre el desempeño y pudiera resultar no aceptable para la organización.

Políticas Relacionadas: “[Ofertas y Aceptaciones Electrónicas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10. Calcomanía de Certificación Antivirus

Política: Los discos flexibles suministrados por entes externos no podrán ser utilizados en los computadores personales ni en los servidores de redes de área local de la Empresa X, a no ser que una persona autorizada haya filtrado y certificado, mediante una calcomanía adherida al disco, que no están contaminados por virus.

Comentario: Esta política provee un certificado que garantiza que todos los discos flexibles suministrados por entes externos han sido verificados para determinar la existencia o no de virus. Esta política también disuade a los usuarios de utilizar sus discos flexibles personales en sus computadores personales del trabajo. Esta política hace que disminuya la confiabilidad en los usuarios finales, ya que se asume que éstos no están capacitados para verificar la presencia de virus. La política asume que una sola persona por departamento o localidad estará autorizada para rastrear virus, la cual será la responsable de colocar las calcomanías en cada disco flexible proveniente de fuentes externas. Las calcomanías deben incluir las iniciales de las personas y la fecha cuando ocurrió la verificación. Si el departamento de compras adquiere continuamente discos

flexibles del mismo color y marca, será más fácil para los auditores internos determinar cuáles provienen de afuera, cuáles fueron verificados y cuándo. Además de los discos flexibles, el alcance de esta política podría ser ampliado para que incluya otros medios de almacenamiento de menor tamaño como CD-ROM, cartuchos óptico-magnéticos, y cintas digitales DAT. Algunas organizaciones llevan esta política un poco más lejos al colocar códigos de barra a sus discos flexibles. Estas organizaciones pueden crear bases de datos que especifiquen el origen, el nombre, la clasificación de sensibilidad y el contenido de cada disco flexible. De esta manera, el cambio de ubicación y el custodio de cada disco flexible pueden ser rastreados automáticamente, y se pueden utilizar los inventarios para conciliar la base de datos con los discos que se tienen físicamente.

Políticas Relacionadas: “[Clasificaciones de Medios de Almacenamiento de Datos](#)” y “[Etiquetado de Clasificación de Datos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Exploración de Software Descargado

Política: Antes de descomprimir el software descargado de fuentes ajena a la Empresa X, éste debe ser explorado por un paquete antivirus autorizado, después de que el usuario haya cerrado su sesión en todos los servidores y eliminado su conexión con otras redes.

Comentario: Esta política muestra a los usuarios cómo protegerse de virus contenidos en el software descargado desde Internet. Esta política elimina la necesidad de que el departamento de Tecnología Informática se involucre en la rutina diaria, y asume que los usuarios están conscientes de encontrarse en ese momento descargando información de Internet, y que tienen información sobre los diferentes virus y su comportamiento. Un nuevo proceso en Internet, que no es más que un servidor de funcionamiento automático, hace que el software cliente sea transferido a una estación de trabajo conectada a Internet, sin que el usuario se entere. Si bien este mecanismo permite un nuevo nivel de funcionamiento en el ambiente cliente-servidor, también representa una amenaza importante en la propagación de virus. Una política como ésta tiende a volverse obsoleta en pocos años, ya que el software para el rastreo de virus realiza todos los pasos definidos en la política.

Políticas Relacionadas: “[Descarga de Software](#)” y “[Transferencia de Archivos Descargados](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Verificación de la Integridad del Sistema

Política: Todos los computadores personales y los servidores de la Empresa X deben ejecutar en forma continua, o por lo menos diariamente, el software de verificación de la integridad de los sistemas para detectar cambios en los archivos de configuración, en los archivos del software del sistema, en los archivos del software de las aplicaciones y en los otros recursos del sistema.

Comentario: El creciente número de nuevos virus informáticos ha disminuido la capacidad de los antivirus tradicionales. Hay tantos virus circulando y creciendo tan rápidamente, que deben hacerse grandes esfuerzos para mantener los antivirus actualizados. Los recientes desarrollos ponen en gran peligro la eficacia del software antivirus que los detecta a través de las secuencias de bits. Hoy en día se necesitan herramientas antivirus más sofisticadas; entre ellas, el método algorítmico y el método heurístico de rastreo. El software para la verificación de la integridad de los sistemas detecta cambios inesperados en el software y en los archivos de configuración, y así impide los cambios o por lo menos da la oportunidad al usuario de detener el proceso de contaminación. Esta política instruye a los gerentes de departamentos locales a utilizar el software antivirus con cierta regularidad, con el objeto de proteger la información y los sistemas informáticos de la Empresa X. Para hacer más llevaderos los esfuerzos en administración y de eliminación de virus, se puede establecer como norma el uso de paquetes antivirus de un proveedor específico. Algunas organizaciones querrán ampliar el alcance de esta política para que mencione las facilidades de detección del comportamiento del virus y su bloqueo. Esta política tiene, además, la capacidad de detectar intromisiones donde ha habido modificaciones a los archivos. Para que un software de verificación de integridad sea eficaz debe estar acompañado de una política que exija que todos los problemas sean reportados inmediatamente.

Políticas Relacionadas: “[Informes de Violaciones y Problemas](#)” e “[Informe de Sospecha de Virus](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

13. Programas Antivirus

Política: Los programas para verificar la presencia de virus, autorizados por el departamento de Seguridad Informática, deben estar activos constantemente en todos los servidores de redes de área local y de los computadores personales conectados a la red.

Comentario: Esta política no establece distinciones entre: los verificadores de la integridad de los programas, los paquetes de rastreo de virus y los paquetes de detección del comportamiento de los virus. En vez de hacer eso, la política depende del departamento de Seguridad Informática para que seleccione uno o más paquetes de software antivirus. El énfasis que esta política pone sobre las máquinas conectadas a la red se justifica ya que los virus u otros programas maliciosos se pueden propagar mucho más rápido en un ambiente conectado a la red que en un ambiente informático independiente. Los computadores que están conectados a la red en forma interrumpida, como los que tienen conexión discada, están conectados a la red para los efectos de esta política. La política hace énfasis en los sistemas de menor escala ya que éstos son los que se contaminan con mayor facilidad. Las palabras "activos constantemente" son utilizadas para indicar que no es suficiente tener el software cargado en el disco duro, sino que debe estar ejecutándose para poder ofrecer la protección necesaria. Muchos cortafuegos incluyen facilidades de verificación de virus. El alcance de la política puede ser ampliado para incluir cortafuegos en ambientes donde los mismos puedan tolerarlos.

Políticas Relacionadas: "Instalación de Software Antivirus," "Sistema de Prueba Antivirus," e "Informe de Sospecha de Virus"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

14. Software Antivirus Actual

Política: Cada trabajador de la Empresa X con responsabilidad de evaluar, procesar o guardar información de dicha empresa utilizando un computador propio, debe instalar y ejecutar regularmente la versión más actualizada del paquete de software antivirus autorizado por el departamento de Seguridad Informática.

Comentario: Esta política garantiza que los trabajadores no perderán datos críticos debido a virus, los cuales entre otras cosas, pueden borrar todo el contenido de un disco duro o insertar palabras incorrectas en documentos escritos. Este requisito no será difícil de cumplir para los trabajadores de la Empresa X debido a

que, si mantienen sus sistemas actualizados, ya tendrán cargados en sus computadores los paquetes de software antivirus más actualizados. La política pasa a ser un apoyo para la comunidad de usuarios si la Empresa X efectivamente suministra el software a los trabajadores. Se recomienda obsequiar este tipo de software con el fin de normalizar varias localidades y facilitar el soporte técnico remoto. El costo del software antivirus disminuye cuando se adquiere en grandes volúmenes.

Políticas Relacionadas: "Múltiples Paquetes Antivirus" e "Información Descargada"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Descifrado de Archivos para Verificar Virus

Política: Todos los archivos legibles por computadores suministrados por entes externos deben ser descifrados antes de ser sometidos a un proceso de verificación de virus autorizado.

Comentario: Muchos usuarios no entienden que algunos virus pueden no ser detectados dentro de archivos cifrados. Los empleados pueden pensar que han actuado conscientemente y que han realizado todas las revisiones para descartar la presencia de virus, pero pueden crear problemas serios de propagación de virus. La política también hace referencia a un proceso autorizado de verificación de virus que puede cambiar con el tiempo a medida que los virus se vuelven más sofisticados. El alcance de la política podría ser ampliado para incluir archivos comprimidos, los cuales no pueden ser verificados adecuadamente por los programas antivirus. Actualmente, los virus pueden encontrarse en ciertos tipos de archivos de datos y en otros materiales informáticos además del software. Esta es la razón de utilizar el término "archivos" en la política.

Políticas Relacionadas: "Eradicación de Virus de Computadores"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

16. Protección Contra Escritura para Software

Política: Aparte de cuando se instala, se reconfigura, o de cuando deba modificarse a sí mismo para funcionar adecuadamente, todo software que se ejecute en computadores personales o en estaciones de trabajo

debe estar protegido contra escritura, de tal manera de generar un mensaje de error si un virus trata de modificarlo.

Comentario: La política establece ciertos parámetros a los computadores personales y a las estaciones de trabajo para que el software no pueda ser modificado sin la específica autorización del usuario. Por ejemplo, si un virus tratara de infectar a un procesador de palabras, el usuario recibiría un mensaje de que la operación de escritura solicitada no puede llevarse a cabo. Esto sería un indicativo de que un virus, o un software no autorizado, ha infectado el sistema. Debido a que el efecto del virus no se evidencia en forma inmediata, sino que se mantiene al acecho, esto se convierte en una importante base de detección. El aspecto resaltante de esta política es su facilidad de implantación y, además, a menudo resulta muy efectiva en la detección de virus y de programas relacionados. Mecanismos sencillos, tales como la pestaña de protección contra escritura en discos flexibles, satisfacen los requisitos de esta política. Algunos paquetes de software requerirán modificarse a sí mismos al momento de instalarse o reconfigurarse, pero luego de esto no existirá la necesidad de repetir esta operación. Después de la instalación inicial del sistema se deben activar las banderas de protección de escritura. De existir la necesidad de modificar los parámetros del sistema más adelante, se procedería a desactivar las banderas de protección contra escritura, se modificarían los parámetros del sistema, y de nuevo se activarían las banderas de protección contra escritura. Con cierto software resulta problemático utilizar protección contra escritura y, por eso, el alcance de esta política podría ser ampliado para profundizar en tales puntos. Es una generalidad aceptada que este enfoque no es una protección adecuada contra los virus, ya que ello requiere de un sistema adicional.

Políticas Relacionadas: ["Informe de Sospecha de Virus"](#)

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

17. Rastreo de Virus en Archivos de Respaldo

Política: Antes de restaurar los archivos de los sistemas informáticos de la Empresa X desde un medio de almacenamiento de respaldo, dichos archivos deben haber sido explorados con la versión más actualizada de software antivirus.

Comentario: Esta política garantiza que los sistemas de producción no se verán afectados por la reentrada de un virus informático. En algunas ocasiones, el personal técnico hará grandes esfuerzos para eliminar un virus de un sistema en particular, sólo para evidenciar que éste se encuentra de nuevo en el sistema a través de un medio de almacenamiento de respaldo. Esto puede ocurrir fácilmente ya que cuando se llevaron a cabo los respaldos, los administradores de sistemas pueden no haber estado en conocimiento de que los archivos estaban contaminados debido a que la versión vigente del software antivirus pudo haber omitido su presencia. Existe mayor probabilidad de que las versiones posteriores del software de rastreo de virus tengan la capacidad de detectar estos virus.

Políticas Relacionadas: ["Control de Acceso para Restaurar Archivos"](#) y ["Descifrado de Archivos para Verificar Virus"](#)

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

18. Asociación con Virus Informáticos

Política: De manera deliberada, los usuarios no deben escribir, generar, compilar, copiar, recolectar, propagar, ejecutar o tratar de introducir código de computación diseñado para auto-rePLICARSE, dañar o de alguna manera entorpecer el desempeño de cualquier computador o red de la Empresa X.

Comentario: Esta política prohíbe específicamente cualquier tipo de relación con los virus. Muy apropiada para el ambiente universitario, donde estas actividades son consideradas de interés académico, esta política afirma que cualquier relación con los virus está fuera de orden. Debido a que los virus son difíciles de contener y de aislar, la propuesta más segura es la de prohibir a los usuarios relacionarse con ellos en forma alguna. La política también elimina la posibilidad de cualquier reclamo por parte de los usuarios, en el que afirmen que la misma organización los alentó a optimizar sus pericias informáticas, y que estos esfuerzos fueron realizados sólo para aprender programación. La palabra "generar" puede parecer innecesaria, pero realmente es diferente de "escribir". Existen varios programas gratuitos que permiten a los usuarios construir sus propios virus.

Políticas Relacionadas: ["Informe de Sospecha de Virus"](#)

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

19. Instalación de Software por Usuario

Política: Los usuarios no deben instalar software en sus computadores personales, en los servidores de red o en otras máquinas, sin haber recibido la previa autorización de un coordinador local de seguridad informática.

Comentario: El acceso a Internet ha puesto un gran número de programas nuevos a la disposición de la población usuaria. Si los usuarios instalan dichos programas o permiten que la instalación se haga a través de una rutina automática de instalación, se podrían propagar los virus o se podrían iniciar fallos en los sistemas y otros tipos de problemas. Esta política prohíbe explícitamente a los usuarios instalar cualquier software sin obtener previamente la autorización del coordinador de seguridad informática. Está disponible software nuevo para computadores personales que evitaría que los usuarios utilicen otro software distinto del autorizado por la gerencia. Esto implica que la política prohíbe el uso de los subprogramas JAVA y Active X, aunque algunos usuarios quizás no lo entiendan.

Políticas Relacionadas:“[Inhabilitación de Java](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

20. Carga de Programas Externos

Política: Los usuarios no podrán instalar en sus computadores personales, estaciones de trabajo, servidores de red o en computadores conectados a la red, ningún programa desarrollado fuera de la Empresa X, a menos que dicho programa haya sido autorizado por el departamento de Seguridad Informática.

Comentario: La política establece un requisito para el control de las modificaciones del software para sistemas de redes distribuidas. Esta política garantiza que ningún software será instalado en los computadores conectados a la red sin haber sido previamente examinado para detectar virus, gusanos y otros códigos no autorizados. Esta política también puede ser utilizada para prohibir el uso de software no autorizado, después de adoptarse un software normalizado a nivel organizacional. Tener el mismo software en toda la red permite al Centro de Atención al Usuario suministrar un mejor apoyo, así como una mejor administración de la red. Algunas organizaciones querrán forzar el cumplimiento de esta

política mediante la utilización de software de inventario. Estos paquetes identifican en forma automática a todos los componentes del software y del hardware en todos los computadores personales o estaciones de trabajo conectados a una red local.

Políticas Relacionadas:“[Exploración del Software](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

21. Actualizaciones Automáticas de Software

Política: No deben efectuarse actualizaciones automáticas de software en los computadores de la Empresa X a través del uso de la tecnología push, a menos que el software utilizado haya sido evaluado por un integrante autorizado del departamento de Sistemas Informáticos.

Comentario: Ciertos proveedores distribuyen las versiones actualizadas de su software sólo a través de Internet. Este tecnología push tiene gran futuro, especialmente para la distribución de versiones actualizadas de software antivirus, aunque también su uso conlleva grandes riesgos; por ejemplo, el no poder utilizar los computadores en una oficina debido a la incompatibilidad entre el software push recientemente cargado y el software existente. Si bien es cierto que los sistemas de actualización para software tipo push ahorrar mucho tiempo a los departamentos de Sistemas Informáticos, los procesos de evaluación de software llevados a cabo por los proveedores pueden no ser mejores que los llevados a cabo por las organizaciones usuarias. Esta política mantiene la estabilidad de los sistemas utilizados por los usuarios al exigir que todo el software que provenga de proveedores sea evaluado antes de ser utilizado dentro de la organización usuaria. En el futuro, cuando los procesos de evaluación de los proveedores se confirmen como adecuados y existan controles de calidad confiables, se podrán hacer excepciones a esta política dependiendo del caso de cada proveedor. Actualmente se deben hacer excepciones en esta política para el software antivirus, ya que cambia muy rápidamente, lo que se aplica igualmente al software de detección de intromisiones.

Políticas Relacionadas:“[Procedimiento de Control de Cambios](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos

22. Descarga de Software Desde Un Sitio Espejo en Internet

Política: El software residente en un sitio espejo en Internet no debe ser bajado a ningún computador de la Empresa X si no es recibido directamente de una fuente conocida y confiable, y sólo si se utilizan herramientas de verificación de software, tales como las firmas digitales.

Comentario: Esta política orienta al personal técnico a ser precavidos en cuanto a la descarga de software desde Internet. Muchos sitios ampliamente conocidos que contienen herramientas para seguridad informática, están duplicados dentro de Internet. Debido a que la integridad del software residente en los sitios espejo es dudosa, el personal que realiza la descarga debe utilizar sólo sitios conocidos y la tecnología de firmas digitales para asegurar que el código no ha sido alterado. Aunque es más riesgoso descargar versiones actualizadas de software desde Internet que comprar un CD-ROM directamente de un proveedor, resulta mucho más rápido y a menudo menos costoso. Dentro de la política se asume que no existen obstáculos para que el personal técnico descargue software, pero dichos obstáculos sí podrían existir para otro tipo de usuarios.

Políticas Relacionadas: “[Descarga de Software](#)” y “[Fuente de Desarrollo de Software](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

23. Descarga de Software por Internet

Política: Los usuarios finales no deben por ninguna razón descargar software de Internet.

Comentario: Esta política le brinda una mayor organización al usualmente caótico entorno de actualización de software de los computadores personales y estaciones de trabajo de los usuarios finales. Los usuarios finales de varias organizaciones están realizando por su cuenta el proceso de actualización de software, lo que a menudo acarrea problemas tanto al Centro de Atención al Usuario como a los que laboran en el área de Sistemas Informáticos. La política asume que la organización ha definido procesos para la distribución de software y sus correspondientes actualizaciones. La política es mucho más eficaz si se pone en práctica con paquetes de control de acceso a las estaciones de trabajo que impidan que los usuarios actualicen software por su cuenta. También es útil para la puesta en práctica de esta política un paquete automa-

tizado para la administración de licencias de software, el cual puede periódicamente llevar un inventario de cuál software está instalado en cada máquina. La política asume que todas las máquinas de los usuarios finales están conectadas a la red local, a una red de área extensa, a intranet o a alguna otra red a través de la cual la actualización de software será difundida de manera activa. Es deseable el retraso ocasionado por la evaluación del software antes de su instalación en toda la organización, ya que permite dar el tiempo para recibir información sobre errores graves reportados en foros públicos. Los responsables de la evaluación de software podrían entonces instalar versiones ya corregidas.

Políticas Relacionadas: “[Descarga de Software Desde Un Sitio Espejo en Internet](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

24. Información Descargada

Política: Todo software y archivos descargados de fuentes ajenas a la Empresa X, a través de Internet o cualquier otra red pública, deben ser explorados con software antivirus, antes de que el software sea utilizado o los archivos examinados por otros programas.

Comentario: Esta política define el proceso que los usuarios deben seguir antes de ejecutar software o abrir un archivo de datos que hayan sido descargados de redes públicas. Antes, los virus, los códigos ocultos y los gusanos eran considerados amenazas para el software, pero hoy en día están siendo incluidos cada vez más dentro de los archivos de datos. Por lo tanto, es necesario filtrar tanto los programas como los archivos de datos. Para evitar la propagación de estos programas no autorizados, la exploración debe llevarse a cabo antes de que cualquier programa sea utilizado. El sitio más efectivo, desde el punto de vista del costo, para tratar con virus o con programas no autorizados es el sitio de entrada a la organización, según lo explica la política. Resulta mucho más costoso manejar estos programas no autorizados una vez se hayan propagado en la organización. Esta política disminuye los efectos negativos generados por los virus y los programas relacionados, los cuales incluyen tiempo de parada de los sistemas, eliminación no autorizada de los archivos de datos y modificaciones imperceptibles a los mismos. Esta política es mucho más fácil de poner en práctica si cada usuario tiene un programa antivirus instalado en su estación de trabajo.

Políticas Relacionadas: “Descarga de Software,” “Descarga de Información Sensible,” y “Exploración del Software”

8.04 Mantenimiento

8.04.01 Respaldo de la Información

1. Copias Maestras del Software

Política: Todo el software de computadores personales debe ser copiado antes de ser utilizado por primera vez, y estos originales deben estar ubicados en un sitio seguro y no deben ser utilizados para las actividades de negocios rutinarias.

Comentario: Esta política garantiza que todos los usuarios tienen originales de respaldo del software que utilizan. Mantener copias del software debe estar incluido en las condiciones de la licencia de uso del software. Muchas licencias permiten tener copias de respaldo, siempre que éstas no sean utilizadas al mismo tiempo que otra copia. Si un grupo de soporte técnico distribuye, actualiza y administra software de computadores personales, entonces no existirá la necesidad de distribuir esta política entre los usuarios finales. El alcance de esta política podría ampliarse para incluir otros tipos de sistemas además de computadores personales (PC), aunque los procedimientos en estos sistemas de mayor tamaño son generalmente más organizados. Algunas organizaciones querrán especificar que las primeras copias del software de producción sean almacenadas tanto cerca como fuera de las instalaciones, en vez de simplemente estar ubicadas en un sitio seguro.

Políticas Relacionadas: “Copias de Software”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Respaldo de Datos

Política: Se debe respaldar mensualmente toda la información de negocio y software crítico residentes en los sistemas informáticos de la Empresa X.

Comentario: Esta política especifica el marco de tiempo mínimo en que puede generarse un respaldo y qué tipo de datos deben respaldarse. Para ciertos tipos de datos el respaldo tiene menor frecuencia, pero estas decisiones dependen del tipo de organización y del tipo de datos, y generalmente deben estar contempladas en el plan de

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

contingencia. Esta política es de mucha importancia para los computadores personales, las redes de área local, los sistemas cliente-servidor y las máquinas de mayor tamaño. Los usuarios de sistemas pequeños a menudo olvidan o tienden a ignorar la necesidad de elaborar los respaldos, lo cual se soluciona en el largo plazo con sistemas de respaldo automático, tales como aquéllos cuyo funcionamiento es transparente para el usuario y se lleva a cabo durante la noche. Dentro de la política se asume que la palabra "crítico" ya ha sido definida.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” y “Proceso de Respaldo”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Medios de Respaldo

Política: Los usuarios deben suministrar sus propios medios de almacenamiento de datos, realizar por cuenta propia el respaldo de los archivos más importantes y nunca utilizar, al elaborar respaldos, los discos duros u otros dispositivos para almacenamiento de datos de los computadores de acceso público de la Empresa X.

Comentario: La política informa a los usuarios que no deben almacenar archivos importantes en máquinas públicas, tales como el laboratorio informático de una universidad o las instalaciones de prueba de una empresa de computación. Debido a que los computadores de los sitios mencionados no poseen controles de acceso, no hay manera de evitar que un usuario modifique o elimine un archivo guardado por otro usuario que haya utilizado estas máquinas. También se recomienda especificar lo que puede esperar un usuario en cuanto a los respaldos llevados o no a cabo. La política también especifica que los administradores de sistemas pueden eliminar en cualquier momento todos los archivos creados por los usuarios, con el objetivo de liberar espacio en disco.

Políticas Relacionadas: “[Respaldos Automáticos](#)” y “[Control de Acceso para Restaurar Archivos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Cifrado en Medios de Respaldo

Política: Debe estar cifrada toda la información sensible, valiosa o crítica registrada en medios de respaldo de computación y conservados fuera de las oficinas de la Empresa X.

Comentario: Los controles de acceso físico existentes en las instalaciones comerciales para realizar respaldos a menudo son de menor calidad que los que posee la organización en su sede principal. Por ejemplo, un candado en un gabinete que contiene medios para almacenamiento de datos puede ser todo lo que está protegiendo los respaldos de la organización. Las instalaciones que albergan los archivos de respaldo a menudo se encuentran desatendidas y accesibles a todo tipo de personal que conforma una organización. Esta política garantiza que sigue existiendo cierto control de acceso a la información sensible, valiosa y crítica conservada fuera de las instalaciones. Para mayor seguridad, algunas organizaciones pudieran solicitar que todos los respaldos estuvieran cifrados, sin tener en cuenta el lugar de almacenamiento de estos respaldos. Esta propuesta, una de las más rigurosas, puede ser la más conveniente para los teletrabajadores, para los que utilizan computadores personales y otros sistemas que hayan sido retirados de las instalaciones de la Empresa X. Hay que tener en cuenta que el cifrado de los datos respaldados hace más lenta o incluso evita la recuperación de los datos. Por ejemplo, en el momento que exista una urgencia de recuperación de datos, puede que no estén disponibles las claves para el descifrado de los medios de respaldo. En esta política se asume que los términos “sensible, valiosa y crítica” han sido ya definidos.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#),” “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#),” “[Información Secreta en Computadores Portátiles](#),” y “[Cifrado de la Información Secreta](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

5. Archivos de Respaldo en Sede

Política: Debe conservarse por lo menos una generación de archivos de respaldo en medios de almacenamiento fuera de línea, sea cual sea la ubicación de los computadores de producción.

Comentario: Esta política facilita una recuperación rápida de todos los archivos de sistemas de producción que hayan sido eliminados por equivocación, dañados por una fractura del cabezal del disquete o contaminados por virus. La disponibilidad inmediata del último respaldo da a los operadores de computación la habilidad de restaurar inmediatamente los archivos dañados, aunque algunas de las últimas transacciones o actualizaciones se pierdan. Esta política protege la información respaldada dentro de las instalaciones contra las actuaciones de los hackers, los saboteadores, los empleados descontentos, los gusanos, los virus y otras amenazas. Si la información está almacenada fuera de línea, será más difícil para los potenciales atacantes acceder a ella. Dada la existencia de un respaldo reciente y de inmediato acceso, los efectos negativos pueden mitigarse.

Políticas Relacionadas: “[Cifrado en Medios de Respaldo](#)” y “[Almacenamiento de Medios de Respaldo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Copias Múltiples de Respaldo

Política: Siempre deben guardarse fuera de las sedes por lo menos dos respaldos recientes y completos realizados en fechas diferentes, contentivos de los registros críticos de la Empresa X.

Comentario: La política garantiza que estará disponible un número adecuado de copias de los respaldos en caso de emergencia o siniestro. Si se utiliza una sola copia, ésta se puede dañar durante su restauración, o al transportarse al centro de restauración. Otro objetivo de esta política es definir un proceso de rotación de los medios físicos de respaldo, que incluya por lo menos dos copias ubicadas fuera de las sedes. La palabra “reciente” es deliberadamente poco precisa, para que la gerencia tenga que interpretar la palabra utilizando la información disponible. Una copia incremental sólo refleja los cambios realizados desde el último respaldo, y su aporte no tiene mayor valor si no se cuenta con el respaldo anterior.

Políticas Relacionadas: “[Copias de Información Sensible, Crítica o Valiosa](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

7. Proceso de Respaldo

Política: Los respaldos incrementales de los archivos de los usuarios finales deben ser realizados por el administrador de turno, desde las 6:00 PM de cada día hábil, con excepción del viernes, día en que se deben realizar respaldos completos de todos los archivos.

Comentario: Esta política explica cuándo deben realizarse tanto los respaldos incrementales como los respaldos totales. Los administradores de redes de área local y el resto de los responsables de la elaboración de respaldos, no pueden argumentar no tener conocimiento de las actividades pendientes. Aunque llevar a cabo un respaldo a las 6:00 PM puede ser engoroso para algunos paquetes de software, dado que algunos archivos pueden estar en uso, muchos paquetes simplemente muestran un indicador de "archivos en uso" y realizan nuevos intentos más adelante. Estos paquetes realizarán varios intentos para respaldar los archivos en uso, y de fallar dichos intentos, se generará una secuencia de comandos que más adelante será ejecutada por un administrador de redes de área local o por otra persona. Lo importante es la periodicidad del proceso, no la hora exacta. Esta política pudiera ser modificada para mencionar que los discos flexibles de respaldo deben ser recolectados por un mensajero, grabados en algún momento, y posteriormente trasladados a un área de almacenamiento fuera de las sedes.

Políticas Relacionadas:["Respaldos Automáticos"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

8. Respaldos Automáticos

Política: Los usuarios con conexión a redes de área local deben dejar sus computadores encendidos durante la noche para la ejecución de los respaldos automáticos.

Comentario: Esta política garantiza que los usuarios finales no apagarán las máquinas, las estaciones de trabajo, los computadores personales u otros computadores con capacidad de almacenamiento local. Los archivos de estos usuarios serán copiados a un servidor local a través de un programa automático de respaldo. Existen razones ecológicas asociadas con esta política, dentro de la cual las palabras "para la ejecución de respaldos automáticos" implican que los controles de

acceso a las estaciones de trabajo deben estar configurados para permitir que se realice el respaldo sin intervención humana alguna. Si se desatiende a una estación de trabajo, los controles de acceso a dicha estación de trabajo, basados en contraseñas, pueden impedir al servidor leer los contenidos del disco duro, salvo que se realice un trabajo adicional. Aunque se recomienda un respaldo automático a un servidor de red local utilizando un software que funcione mediante un temporizador, puede ser necesario ejecutar un software adicional para controlar el acceso a las estaciones de trabajo conectadas a la red que quedan desatendidas. Estas medidas son vitales si la red de área local tiene enlaces externos de comunicación a través de cortafuegos de Internet o mediante un grupo de modem de discado. Las palabras "red de área local" podrían ser reemplazadas por la palabra "intranet".

Políticas Relacionadas:["Control de Acceso a Computadores de Red"](#)

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

9. Revisión de la Información Respaldada

Política: Todos los archivos y los mensajes almacenados en los sistemas de la Empresa X son rutinariamente copiados en cinta, disquete u otro tipo de almacenamiento y deben ser recuperables para su posterior revisión por parte de los administradores de sistemas y otras personas designadas por la gerencia.

Comentario: Esta política, que también versa sobre la privacidad, notifica a los usuarios que su información puede ser examinada por los administradores de sistemas, los investigadores de seguridad y otras personas autorizadas por la gerencia. Esta política podría ser ampliada para mencionar que los mensajes de correo electrónico, las actividades de los protocolos de transferencia de archivos por Internet y otras acciones pueden ser registradas y respaldadas. La política indirectamente sugiere a los usuarios no guardar información sensible en los sistemas de la Empresa X. Si bien esta política puede parecer obvia para los conocedores, la idea detrás de ella quizás no lo sea tanto para los que recién se inician en el área informática, porque los sistemas de respaldo pueden servir como pruebas incriminatorias de cosas que los usuarios pensaron haber destruido. Esta política podría estar acompañada por otra política relacionada que indique en qué momento cifrar los datos.

Políticas Relacionadas: “Transmisión de Datos Secretos,” “Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización,” y “Manejo de Mensajes de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Archivos Críticos de Respaldo

Política: Los datos críticos que hayan sido respaldados no deben ser utilizados para efectos de restauración, a menos que se cuente con otra copia de respaldo de los mismos datos en otro medio de almacenamiento de computación.

Comentario: Esta política garantiza que la única copia vigente de datos críticos o cruciales no será dañada o destruida en el proceso de restauración. La política motiva a los usuarios a realizar una copia adicional de dichos datos, previo al trabajo de restauración. Este enfoque es recomendable porque los sistemas a donde se deban restaurar los datos pueden estar contaminados por virus, gusanos, códigos ocultos u otros tipos de software malicioso. En el proceso de restauración de un archivo, los mismos medios de almacenamiento pueden ser alterados, distorsionados o modificados sin autorización alguna. Asimismo, el hecho de elaborar una copia adicional de datos en otro medio de almacenamiento diferente a la máquina en la cual van a ser restaurados, puede activar el software malicioso. Tener una copia de respaldo adicional es recomendable porque, durante la restauración, el técnico puede cometer errores e inconscientemente eliminar o contaminar el medio físico de respaldo. Como mejor alternativa a elaborar una copia adicional antes de la restauración, se sugiere generar dos copias al momento de realizar el primer respaldo. Se asume dentro de la política que la palabra “críticos” ya ha sido definida.

Políticas Relacionadas: “Copias de Información Sensible, Crítica o Valiosa” y “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

11. Respaldo Antes del Procesamiento

Política: Los procesos de producción por lotes no deben iniciarse hasta que haya finalizado el respaldo de todos los archivos maestros y de las bases de datos maestras.

Comentario: Esta política evita que la organización se encuentre en una situación engorrosa al momento de iniciar sus actividades al día siguiente. Si no se aplica el control establecido en esta política, y de haber fallado el procesamiento en lotes la noche anterior por no contar con la presencia de un operador de guardia que reiniciara el proceso adecuadamente, los trabajadores no estarían en capacidad de acceder a los registros de los clientes ni a otros datos de producción al iniciar sus actividades a la mañana siguiente. Puede que esto se deba a que los registros han sido parcialmente alterados y que no están listos para su uso hasta que finalice el procesamiento en lote. En algunas organizaciones, sería recomendable que los trabajadores tuvieran acceso a las versiones de archivos y de bases de datos no actualizadas por dichas operaciones. Otro de los objetivos de la política es garantizar a la organización interesada en aplicar dicha política, la disponibilidad de una copia del respaldo de los archivos de producción y de las bases de datos críticos, en el caso de que estos sufrieran daños irreparables durante el procesamiento en lote. También es importante tener respaldo de los datos críticos antes del inicio del procesamiento, ya que estos procesos pueden tomar tiempo y consumir gran cantidad de recursos. Este respaldo pre-procesamiento debe hacerse conjuntamente con el respaldo nocturno de rutina que podría llevarse a cabo una vez concluidos el procesamiento en lote y los otros procesos de producción del día.

Políticas Relacionadas: “Respaldo de Datos” y “Validación de Datos de Entrada y Manejo de Item Rechazado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Almacenamiento de Medios de Respaldo

Política: La información de negocios indispensable y los respaldos de software deben ser almacenados en un sitio aislado de la intemperie, con controles de acceso y a una distancia prudencial de la sede donde fueron generados.

Comentario: Esta política garantiza que los respaldos de la información crítica no serán destruidos por siniestros locales tales como accidentes aéreos, detonaciones de bombas o derrames químicos. En vez de especificar que la información debe estar a una cierta distancia de donde fue generada, la política permite que la gerencia local decida qué tan lejos deben estar almacenadas las copias, lo cual puede ser de 8 a 160 km de distancia. Para algunas organizaciones será

suficiente mantener copias vigentes de los respaldos en el sitio en el cual fueron generadas y las otras copias a unas pocas cuadras de distancia. En otros casos, la decisión sobre la distancia a considerar puede estar influenciada por ciertas características locales como el que la zona donde vaya a estar guardada la información sea una zona sísmica. Algunas organizaciones podrían optar por definir una distancia mínima específica con la intención de no repetir en la zona de almacenamiento los mismos problemas que afectan a la zona donde se generó la información. Mientras más alejado se encuentra el sitio de almacenamiento, más costoso y largo será el proceso de recuperación de los respaldos. Este último detalle se puede eliminar con el resguardo electrónico, el cual permite transmitir el respaldo en tiempo real a un sitio remoto a través de Internet.

Políticas Relacionadas:“[Cifrado de la Información Secreta](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

13. Distintas Zonas de Riesgo de Incendio

Política: Los medios de almacenamiento para los respaldos de computación y de redes deben estar ubicados en zonas de riesgo de incendio diferentes a las de las máquinas que generaron los respaldos.

Comentario:La política crea distancia entre los medios utilizados para generar los respaldos y la máquina que los produjo. En lugar de exigir que los medios de almacenamiento estén ubicados fuera de las instalaciones, o a unos cuantos kilómetros de distancia, la política menciona zonas de riesgo de incendio aisladas las unas de las otras, de manera de reducir la probabilidad de que ambas se vean afectadas por el mismo incendio. Edificios distintos dentro de la misma área corporativa pueden estar en diferentes zonas de riesgo de incendio. Igualmente, algunas de las partes que conforman un edificio alto pueden estar dentro de zonas de riesgo diferentes. Debido a que los detalles de un edificio siempre serán diferentes, esta política obliga al uso de la zona de riesgo de incendio, dejando el resto al departamento de Seguridad Física. Para mayor protección, un sistema de rotación de medios de almacenamiento podría rotar los medios de almacenamiento entre las distintas zonas de riesgo. Algunas organizaciones querrán ampliar el alcance de esta política, exigiendo que se almacene periódicamente una copia lejos de la máquina utilizada para elaborar el respaldo.

Políticas Relacionadas:“[Almacenamiento de Medios de Respaldo](#)” y “[Cifrado en Medios de Respaldo](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

14. Almacenamiento de Medios de Respaldo

Política: Todas las áreas a prueba de incendios utilizadas para el almacenamiento de medios de respaldo incluyendo, sin limitantes, los depósitos, las bóvedas y los gabinetes, deben mantenerse completamente cerradas cuando no estén en uso, a no ser que posean un mecanismo de cierre que dispare una alarma contra incendios.

Comentario:Esta política garantiza que la tecnología a prueba de incendios funcionará de la manera diseñada originalmente. Si el personal de operaciones informáticas deja abierta la puerta de un gabinete a prueba de incendios que alberga el respaldo semanal y se produce un incendio, el gabinete no podrá brindar ningún tipo de protección a los respaldos. Si existe algún tipo de seguridad adicional, tal como un candado en las bóvedas y en los gabinetes a prueba de incendio, puede aprovecharse para controlar el acceso.

Políticas Relacionadas:“[Resistencia al Fuego de Centros de Computación](#)” y “[Areas Desatendidas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

15. Archivos de Sitios Web y Comerciales

Política: Todas las versiones de los archivos de los sitios web de Internet y sitios comerciales deben estar archivados de manera segura en dos lugares físicamente separados.

Comentario:Esta política crea un archivo redundante de cada versión de los sitios web de Internet y sitios comerciales, porque puede ser de mucha importancia para fines legales. Por ejemplo, si existiera un conflicto legal relacionado con una oferta publicada en un sitio web, y si la integridad de los datos y los controles de acceso fuesen parte del proceso de archivado, estos registros podrían utilizarse para probar sin lugar a dudas cuál fue la información publicada en el sitio web. Un banco podría utilizar un archivado como éste para resolver un conflicto relacionado con las tasas de interés ofrecidas para ciertos tipos de cuentas de ahorro o certificados de depósito, así como también podrían utilizarse para planes de contingencia cuando, por

ejemplo, una organización que brinda servicios de hospedaje de sitios web destruye todas las copias del sitio. Debido a que tantas organizaciones utilizan sitios de hospedaje externos, es importante que vigilen al proceso de archivado de sus respaldos. En algunas jurisdicciones pueden incluso existir razones legales para mantener copias de los sitios Internet.

Políticas Relacionadas: “[Respaldo de Datos](#)” y “[Manejo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

16. Respaldo de Información Crítica

Política: La información empresarial de carácter crucial o crítico, así como el software crítico, debe respaldarse por lo menos trimestralmente en medios de almacenamiento de archivo y retenerse por lo menos durante un año.

Comentario: Esta política reconoce que los virus y los códigos ocultos pueden alterar los archivos y que estas alteraciones pueden no ser detectadas durante largo tiempo. Esto significa que varias generaciones de respaldos pueden contener archivos contaminados o alterados, y que los entes responsables no están al tanto del problema hasta que todos los respaldos que hayan sido rotados estén contaminados o sobrescritos. Al enfrentarse con este tipo de situaciones, las únicas esperanzas para el software pueden ser los medios de almacenamiento de la instalación original, o el proveedor o el agente custodio. Posiblemente se haya modificado erróneamente la información crítica de negocio, y dichas modificaciones pueden permanecer ocultas por mucho tiempo. Asimismo, de no ser aplicada una política como ésta, todos los respaldos podrían contener información fraudulenta. De no aplicar el proceso descrito en esta política, puede ser muy difícil o imposible recuperar la información original. El costo de esta política es bajo cuando las operaciones de respaldo están automatizadas. El alcance de esta política puede ser ampliado con una política que especifique cuándo y cómo deben destruirse estos respaldos archivados. La asesoría legal de la corporación debe ser consultada en lo relativo a los asuntos legales.

Políticas Relacionadas: “[Copias Múltiples de Respaldo](#)” y “[Respaldo de Datos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Directorio de Almacenamiento de Archivos

Política: Todos los datos de respaldo archivados y almacenados fuera de las instalaciones deben estar reflejados en un directorio actualizado, que especifique la fecha más reciente de modificación de la información y la naturaleza de la misma.

Comentario: Esta política facilita la decisión en cuanto a conservar o no cierta información en archivos de almacenamiento, y de ser así, su ubicación específica. En algunos de los sistemas de manejo de almacenamiento de archivos, los archivos son trasladados automáticamente entre cintas magnéticas, unidades de disco, y otros medios, basado en la última fecha en que fueron accedidos. Un directorio de los archivos y de su ubicación se genera automáticamente como subproducto de la actividad del sistema. Estos directorios también pueden ser actualizados manualmente, aunque tanto el nivel de esfuerzo como las probabilidades de cometer errores son mayores que cuando están automatizados. Un directorio como éste resulta útil cuando existe un conflicto legal. Dicho directorio puede ser igualmente utilizado por la contraparte en un litigio legal para identificar documentos que pudieran ayudar en su argumento; así como puede ser utilizado para planes de contingencia y para la preparación de reclamos de seguros. Este directorio constituirá un elemento instrumental en los procesos de purga que se lleven a cabo.

Políticas Relacionadas: “[Destrucción de Información](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

18. Medios de Almacenamiento de Archivos

Política: Los medios en los cuales se almacene información sensible, valiosa o crítica por períodos de tiempo superiores a seis meses, no deben estar sujetos a una rápida degradación.

Comentario: Esta política especifica los medios de almacenamiento en los cuales deben resguardarse los registros importantes. La situación ideal sería utilizar el mismo medio de almacenamiento a lo largo de toda la organización; por ejemplo, un cartucho de cinta magnética de un tamaño específico para el respaldo de computadores portátiles. Utilizar medios de diferentes tamaños, formatos, y tipos, resultará en una difícil o imposible recuperación de la información almacenada. Pueden ser suministrados, como parte de la política, muestras de medios de almacenamiento aceptables, tales como CD-ROM y papel para libros libres de ácido. Esta

política resulta innecesaria si la organización sólo utiliza medios de almacenamiento adecuados para archivado. En la política se asume que las palabras "sensible, valiosa, o crítica" han sido ya definidas en otro documento.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías," "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones," "Inspección de Bolsos," y "Prevención del Copiado de Documentos Sensibles"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

19. Pruebas de Medios de Almacenamiento de Archivos

Política: Tanto la información crítica de negocio como el software crítico archivados en medios de almacenamiento de computación por un largo período de tiempo, deben probarse por lo menos una vez al año.

Comentario: Esta política garantiza que los datos archivados serán fácilmente recuperables en el momento que sea conveniente. De sobrevenir inconvenientes, deben realizarse esfuerzos rápidos para transferir los datos a medios de almacenamiento más seguros. Como ejemplo de estos inconvenientes, se puede mencionar la información almacenada en cintas magnéticas las cuales tienden a crear errores con el tiempo. Estos datos pueden ser transferidos a un CD-ROM, el cual puede funcionar por muchos años. Esta política puede ser fundamental en la identificación de los problemas asociados con un sitio de almacenamiento, con procedimientos relacionados y con un software relacionado. Por ejemplo, puede que haya demasiado polvo en el área de almacenamiento, y esto puede interferir en la recuperación de ciertos datos almacenados en cintas magnéticas legibles por el computador. Si estos problemas no han sido identificados por la gerencia, la política puede hacerlos salir a la luz.

Políticas Relacionadas: "Calidad de los Medios de Almacenamiento de Archivos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

20. Calidad de los Medios de Almacenamiento de Archivos

Política: Los medios para almacenamiento de datos de computación utilizados para almacenar información sensible, crítica o valiosa, deben ser de alta calidad y puestos a prueba en forma periódica.

Comentario: Esta política exige que sólo se utilicen medios confiables para el almacenamiento de datos. No se puede confiar en medios antiguos y desgastados para el almacenamiento adecuado de la información. Muchas organizaciones grandes tienen máquinas dedicadas para situaciones especiales para poner a prueba los medios donde será almacenada la información. Si las máquinas determinan que los medios contienen muchos errores, los medios deben ser eliminados de los respaldos. Los usuarios finales generalmente no cuentan con el equipo idóneo para poner a prueba detalladamente los medios para almacenamiento de datos, pero sí pueden calificar la calidad de los discos flexibles para lectura y escritura, así como determinar que los medios de almacenamiento ya no son confiables. Dentro de la política se asume que las palabras "sensible, crítica, o valiosa" ya han sido definidas en otros documentos.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías," "Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones," y "Pruebas de Medios de Almacenamiento de Archivos"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

21. Preservación del Almacenamiento de Archivos

Política: La integridad de la información sensible, crítica o valiosa, almacenada por largos períodos de tiempo, debe estar garantizada por procedimientos para el almacenamiento de medios de computación.

Comentario: Esta política insta a la gerencia a tomar las medidas necesarias para la conservación de los datos almacenados en archivos, en los casos en que los datos se estén deteriorando o a punto de deteriorarse. Esta política puede ser ampliada para que se permita la transferencia de datos a medios más actualizados para el almacenamiento de datos. Por ejemplo, los datos que se encuentren almacenados en tarjetas perforadas, pueden ser transferidos a cintas magnéticas para aumentar su accesibilidad y su conservación. Igualmente, los datos plasmados en un papel en mal estado pueden ser transferidos a medios más seguros de almacenamiento.

En esta política se asume que las palabras "sensible, crítica o valiosa" ya han sido definidas en otros documentos.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#),” “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#),” “[Medios de Almacenamiento de Archivos](#),” y “[Pruebas de Medios de Almacenamiento de Archivos](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

22. Formularios de Papel Almacenados Fuera de Sede

Política: Los formularios en papel almacenados fuera de las sedes, deben ser puestos a prueba por lo menos cada tres meses para comprobar su compatibilidad con las impresoras, las máquinas de fax y otros equipos de la Empresa X.

Comentario: Esta política garantiza que los formularios almacenados fuera de sede no serán relegados hasta el momento de una emergencia o un siniestro, ya que para entonces puede ser muy tarde para reemplazar los formularios por otros compatibles con el equipo en uso. Resulta más difícil conseguir formularios impresos que el papel normal de impresora o de fax. Este retardo en el proceso de obtención del papel implica que hay que poner un interés especial en la administración de los formularios. Esta política acepta el hecho de que los formularios son perecederos y que por lo tanto deben ser puestos a prueba en forma periódica, ya que no es suficiente una inspección visual.

Políticas Relacionadas: “[Calidad de los Medios de Almacenamiento de Archivos](#)” y “[Calidad de los Medios de Almacenamiento de Archivos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8.04.02 Registros de Operadores

1. Registros de Operadores de Computadores

Política: Todos los sistemas multiusuario de producción de la Empresa X deben poseer registros de los operadores de computadores que muestren los períodos de arranque y de parada de las aplicaciones de producción, los períodos de arranque y de reinicio de los sistemas, los cambios a la configuración de los sistemas, los errores de los sistemas y sus acciones correctivas, y la confirmación de que los archivos y las salidas fueron manejados correctamente.

Comentario: Esta política garantiza que todos los sistemas multiusuario de producción poseen un registro de operadores, que puede servir de apoyo en la resolución de problemas. Los registros también pueden ser útiles en las investigaciones relacionadas con fraudes, malversación, sabotaje, espionaje industrial u otros incidentes relacionados. Asimismo, los registros pueden garantizarle a la gerencia que los operadores están siguiendo las instrucciones correctamente. Esta garantía es de suma importancia ya que los operadores pueden ocasionar algún tipo de daño. Los detalles que se incluyen en un registro de operaciones pueden ser omitidos en la política y ser reemplazados por las palabras "detalles operacionales especificados por el gerente de Operaciones de Computación". Este último enfoque permite modificar los detalles sin tener que modificar la política. Este enfoque permite que se

utilicen diferentes tipos de registros para diferentes sistemas operativos. Encender o apagar un registro puede ser considerado una reconfiguración del sistema, y no se especificó como tal en la política. Esta política resulta importante para servidores de redes de área local, servidores comerciales de Internet, servidores de intranet y otros sistemas multiusuario de producción.

Políticas Relacionadas: “[Actualización de Información de Producción](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Revisión de Registros de Operadores de Computadores

Política: Todos los registros de los sistemas multiusuario de producción de la Empresa X deben ser revisados con regularidad por el gerente de Operaciones de Computación o por el especialista designado por el gerente de Sistemas Informáticos.

Comentario: Esta política tiene la intención de garantizar que los operadores seguirán las instrucciones establecidas en los procedimientos, y que son responsables de sus actos en relación con los sistemas de producción. Si se llevan registros, pero nunca se revisan,

serán menos efectivos como elementos disuasivos contra el abuso por parte de los operadores. Asimismo, sin inspecciones regulares, algunos gerentes repararán en algunos problemas sólo cuando éstos necesiten atención inmediata. El responsable de revisar los registros no debe ser un operador informático. La necesidad de designar a alguien para revisar los registros es particularmente obvia en un entorno informático distribuido donde puede no haber un gerente de Operaciones de Computación y la actividad

puede ser pasada por alto. Una política como ésta es necesaria, ya que este tipo de actividad tiende a ser relegada por otras de mayor urgencia.

Políticas Relacionadas: “[Revisión de Registros del Sistema](#)” y “[Registros de Operadores de Computadores](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

8.04.03 Registros de Fallas

1. Informes de Problemas

Política: Debe existir un proceso formal para el manejo de problemas, de tal modo que éstos puedan quedar registrados para minimizar su incidencia y evitar que ocurran de nuevo.

Comentario: Esta política requiere que los usuarios puedan establecer diferencias entre los efectos que ciertos problemas tienen sobre sus datos y la calidad de servicio que reciben. Al entender la naturaleza de los problemas, los usuarios pueden apreciar el servicio que reciben y la integridad de los datos que utilizan en la toma de decisiones. Otro objetivo de esta política es

tener establecido y operativo un sistema de manejo de problemas. Estos sistemas pueden ser utilizados como herramientas para el reporte y la resolución de problemas de seguridad, tales como la contaminación por virus o el uso no autorizado de los sistemas.

Políticas Relacionadas: “[Reportes Externos de Violaciones](#),” “[Informes de Violaciones y Problemas](#),” y “[Mantenimiento Preventivo](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8.05.01 Controles de las Redes

1. Relaciones de Confianza entre Servidores

Política: A menos que la gerencia de Seguridad Informática lo haya autorizado por escrito, el personal de la Empresa X no puede permitir que exista ningún tipo de relación de confianza entre los computadores conectados a la red interna de la Empresa X.

Comentario: Esta política advierte a los administradores de sistemas y de seguridad que no deben utilizar ninguna relación de confianza entre los computadores de la red interna de la Empresa X. Estos sistemas permiten que un usuario se conecte a una máquina y acceda a los archivos almacenados en otra. Si un hacker lograra entrar a una de las dos máquinas con este tipo de sistema instalado, podría fácilmente sabotear o utilizar las dos máquinas sin mayor esfuerzo. Es mucho más seguro que cada usuario se conecte a cada máquina por separado.

Políticas Relacionadas: “[Sistemas de Directorios Compartidos](#)” y “[Mal Funcionamiento del Control de Acceso](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Configuración de Seguridad

Política: Los parámetros de configuración y de instalación de todos los servidores incorporados a la red de la Empresa X deben ajustarse a las políticas y normas de seguridad internas.

Comentario: Esta política establece que todos los administradores de seguridad, de sistemas, de redes, y cualesquiera otros trabajadores encargados de administrar los sistemas de seguridad, deben regirse por las políticas y las normas internas de manejo de sistemas de seguridad. A menudo, estos administradores hacen las cosas a su manera, al permitir en forma inadvertida un

acceso no autorizado a máquinas conectadas. Esta política puede parecer innecesaria, pero tiene su mérito establecerla por escrito y con ello permitir que la gerencia exija los administradores que se rijan por las políticas y normas de la Empresa X.

Políticas Relacionadas: “[Convenciones en Desarrollo de Sistemas](#)” y “[Código de Conducta Corporativo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Interfaces a Redes Externas

Política: Los diseñadores y desarrolladores de los sistemas de la Empresa X deben restringir la utilización de las interfaces de redes y protocolos externos y utilizar aquéllos expresamente autorizados por la gerencia de Seguridad Informática.

Comentario: Esta política impide que los diseñadores y desarrolladores codifiquen software con interfaces y protocolos nuevos para los cuales no existe validación de seguridad sólida, confiable y operacionalmente manejable. La política evita también el uso de interfaces y protocolos de dudosa efectividad, que vienen en los paquetes del software que la organización ha comprado, alquilado o arrendado. El uso de interfaces o protocolos nuevos, o de interfaces o protocolos desactualizados, supedita la organización a una variedad de vulnerabilidades desconocidas. Las interfaces y los protocolos más comunes por lo menos han sido evaluados detalladamente y puestos a prueba en forma permanente y completa. Con esta política se minimiza el uso a sólo las interfaces y los protocolos más aceptados. Otra función de esta política es la promoción de la normalización de las interfaces y de los protocolos de redes internas, lo que facilita el establecimiento de sistemas centralizados para la administración de redes. La política se abstiene en forma deliberada de comentar sobre Internet, así que también es aplicable a otros tipos de redes externas.

Políticas Relacionadas: “[Sistemas en Interface con Redes Externas](#)” y “[Autentificación del Usuario por el Sistema Operativo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Revisión de Conexiones Remotas

Política: La Empresa X debe monitorear rutinariamente los computadores personales conectados a sus redes para detectar virus, mediante el uso de software autorizado y con licencia, al tiempo de monitorear la actividad generada desde estos sistemas.

Comentario: Esta política notifica a los usuarios remotos que la Empresa X posee y utiliza software para monitoreo y control remoto. Muchos usuarios no conocen la existencia de dicho software o que su empleador está utilizando un software que controla sus computadores desde sitios remotos y esta política previene a dichos usuarios sobre esta posibilidad. También los previene en cuanto a que el contenido y la configuración de sus sistemas pueden estar siendo examinados por personal de la Empresa X. La política, en forma indirecta, desalienta el uso de los sistemas de manera personal, o en una forma no aprobada por la gerencia de la Empresa X. Esta política evalúa los archivos del explorador, el archivo histórico del explorador que muestra los sitios visitados en la red y los archivos guardados en el disco duro. En esta política se supone que sólo los computadores suministrados por la Empresa X pueden estar conectados a su red interna. De prevalecer otro enfoque en el entorno, entonces se puede modificar la política.

Políticas Relacionadas: “[Monitoreo de Contenido de Correo Electrónico](#)” y “[Correo Electrónico del Departamento de Ventas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

5. Control de Tráfico en Internet

Política: La Empresa X debe monitorear el tráfico en Internet sin bloquear ni filtrar los sitios visitados por los trabajadores, ni censurar las transmisiones enviadas o recibidas.

Comentario: Esta política notifica a los usuarios que sus visitas a Internet están siendo controladas. Legalmente hablando, algunas jurisdicciones exigen estas notificaciones si la gerencia tiene la necesidad de acceder a esta información con fines disciplinarios. Esta política no requiere de ningún paquete de software especial para controlar la navegación en Internet ni de personal adicional para realizar el trabajo. La política sólo especifica que las navegaciones en Internet serán controladas por la gerencia y, en este caso, la política servirá de elemento de disuasión, más que cualquier otra cosa. Los usuarios son libres de navegar en Internet, pero

cualquier conducta abusiva será manejada con estrictas medidas disciplinarias. El uso de esta política, sin mayores explicaciones de lo que significa una conducta abusiva, no constituye por sí misma una justificación para prohibir el acceso de un usuario a Internet. El uso de esta política está más orientado hacia adiestrar a los usuarios a prestar atención a su trabajo, y a no distraerse con sitios en la Internet que no están relacionados con su trabajo, grupos de intereses comunes, estaciones de radio, y cualquier otro servicio disponible en Internet.

Políticas Relacionadas: “[Monitoreo de Actividad en Internet](#)” y “[Etiquetas de Contenido en Internet](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Cookies

Política: Antes de que se utilicen cookies y en cualquiera de los sitios web y comerciales de la Empresa X, se debe demostrar de manera convincente la necesidad de recolectar datos confidenciales ante el comité gerencial de Seguridad Informática, el cual además debe autorizar tal uso.

Comentario: Esta política impide que la gerencia invada la privacidad, aunque sea en forma no intencional. En algunas organizaciones, los técnicos establecen sistemas web que realizan funciones no entendidas por la gerencia y, por ende, no autorizadas por ella. Esta política garantiza que los cookies, a los cuales antecede una mala reputación dentro de la comunidad protectora de la privacidad, sólo serán utilizados en caso de extrema necesidad. La organización debe divulgar el uso de dichas tecnologías en caso de que las utilice. Los cookies pueden ser transparentes para los usuarios, aunque algunos exploradores nuevos pueden estar configurados para preguntar al usuario si aceptan el uso de un cookie de un sitio en particular. La mayoría de los sitios colocan cookies en las máquinas de los usuarios a nombre de organizaciones de mercadeo de terceros, y estos mismos dispositivos se utilizan luego para rastrear y preparar informes sobre las actividades de los usuarios.

Políticas Relacionadas: “[Cookies en Internet](#)” y “[Cookies para Inicios Automáticos de Sesión](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Esconder Transmisión de la Información

Política: Toda información considerada sensible, de fácil acceso a través de medios públicos y que pueda ser de utilidad para los adversarios, debe ser ligeramente modificada con el objeto de esconder su real naturaleza de alta integridad.

Comentario: Esta política especifica los mecanismos para suministrar información útil para todo tipo de público, pero sin ser de tan alta calidad como para ser utilizada por parte de los adversarios. A manera de ejemplo se pueden tomar las transmisiones de los sistemas de posicionamiento global y de horario suministrados por satélites. Los satélites militares pueden haber definido estas señales en forma tan precisa, que fuerzas extranjeras pudieran utilizar esta información para guiar sus misiles nucleares. Así que la versión cifrada de estas señales puede estar disponible sólo para los sistemas militares probablemente con un exceso cifrado para aislar la información importante de la información extraña, aunque de todas maneras, el público tenga la necesidad de acceder a esta información para orientar botes y aeronaves. La solución pudiera estar en utilizar una versión ligeramente modificada y de fácil acceso en forma de lectura para este público. Aunque esta política resulta de mayor importancia para los sistemas militares y gubernamentales, también pudiera ser de interés comercial. El enfoque anterior pudiera ser de interés para las organizaciones comerciales, en situaciones en las cuales tuvieran que mantener información tanto en forma confidencial como abierta al público. En dichos casos, sería recomendable elaborar resúmenes de esta información sensible.

Políticas Relacionadas: “[Restricciones a la Recopilación de la Información](#),” “[Protección de Mensajes Cifrados](#),” y “[Confiabilidad de la Información de Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

8. Punto Central de Falla de la Red

Política: La gerencia debe diseñar las redes de comunicaciones de la Empresa X de manera tal que no exista un solo punto central de falla que pudiera causar la no disponibilidad de los servicios de la red.

Comentario: Esta política sirve de guía para los diseñadores de sistemas, los técnicos en redes y otros de manera tal que puedan construir los sistemas que aspira la gerencia. Fallas recientes y muy publicitadas del

sistema telefónico evidencian la dependencia que tienen las organizaciones de sus redes. Esta política implica el hecho de que el departamento responsable de las telecomunicaciones debería conseguir por lo menos dos operadoras de telecomunicaciones de larga distancia, conexiones temporales vía microondas en caso de que las líneas en tierra queden fuera de servicio y cualquier otra alternativa redundante. Si bien no es realizable de inmediato, la política funciona como objetivo al cual aspira la mayoría de las organizaciones. En la política se utilizó el término "no disponibilidad" en vez de "interrupción". Si parte de una red interna queda fuera de servicio, se puede esperar una disminución temporal de la calidad de servicio de la red, pero la mayoría de las empresas le da mayor importancia a la disponibilidad de la red que a la degradación de la calidad del servicio. Una evaluación de riesgos podría indicar un resultado diferente, por lo que sería conveniente modificar la terminología utilizada.

Políticas Relacionadas: “[Múltiples Operadoras Telefónicas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Múltiples Operadoras Telefónicas

Política: La gerencia debe diseñar los sistemas de comunicaciones de la Empresa X de tal modo que las comunicaciones críticas sean enviadas inmediatamente mediante varias operadoras de telecomunicaciones y a través de rutas físicamente diferentes.

Comentario: Fallas mayores en las líneas telefónicas de larga distancia han demostrado que es recomendable que las organizaciones tengan por lo menos dos compañías operadoras de larga distancia. Esta política es una guía administrativa definitiva para los responsables del manejo de los sistemas de comunicaciones. La política abarca tanto las redes de voz como las redes de datos, y se aplica sólo a las comunicaciones críticas. En la política se asume que la palabra "crítica" está definida en otra política.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Punto Central de Falla de la Red](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Registros de Nombres de Dominio en Internet

Política: Los pagos y la documentación para el registro de los nombres del dominio de Internet para los sitios oficiales de la Empresa X deben ser manejados a tiempo y confirmados de inmediato por el gerente de Telecomunicaciones.

Comentario: Esta política impide interrupciones innecesarias dentro de la actividad del sitio y comercial en Internet. Los sitios de grandes organizaciones ampliamente conocidas han quedado fuera de servicio por largos períodos de tiempo por no haber pagado sus facturas a tiempo. Aunque muchas empresas no lo crean, actualmente sucede que un ente autorizado desconecta los sitios comerciales y web de dichas empresas cuando los pagos no se reciben a tiempo.

Políticas Relacionadas: “[Mantenimiento de Equipos](#),” “[Nombre de Dominio en Internet](#),” y “[Mantenimiento Preventivo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Herramientas para Evaluar Integridad

Política: Todos los sistemas conectados a Internet utilizados con fines productivos, deben usar diariamente herramientas para evaluar la integridad de los archivos y comparar las firmas digitales de los archivos críticos con las firmas digitales mantenidas en un sistema desconectado.

Comentario: Esta política requiere que los sistemas conectados a Internet tengan un sistema de evaluación de la integridad de los archivos que detecte cambios en los archivos críticos. En la política se asume que los hackers, los ex-empleados descontentos, la competencia y otros intrusos podrán traspasar el cortafuego y otras medidas de seguridad. Esta siguiente línea de defensa puede no sólo restaurar las versiones autorizadas de diversos archivos, sino también detectar cambios en los mismos y, de este modo, exigir una investigación. Este enfoque no será efectivo para aquellos archivos que sufren muchas modificaciones, sino para aquellos relativamente estáticos, tales como los archivos de configuración del sistema. La utilización de sistemas desconectados impide que los intrusos modifiquen las firmas digitales preservadas en las máquinas de referencia. Un sistema de evaluación de la integridad de los archivos puede ser utilizado para detectar las

ocasiones en las cuales los desarrolladores de sistemas o personal técnico de soporte han llevado a cabo cambios sin tener la autorización para hacerlo.

Políticas Relacionadas: “[Remoción de Registros de Computadores Accesibles desde Internet](#)” y “[Verificación de la Integridad del Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Servicios de Protección de Mensajes en Red

Política: Al suministrar el servicio de redes de computación, la Empresa X no debe suministrar servicios de protección de mensajería.

Comentario: Esta política es para aquellos suscriptores que utilizan la red de la Empresa X y para terceros con los cuales la Empresa X se comunica a través de la red. En algunos casos, esta política o una derivada puede ser importante para aquellas organizaciones que soportan a un servidor en Internet que remite correos o suministra servicios a la amplia comunidad Internet. La política limita las responsabilidades que tiene la Empresa X en lo relativo a medidas de seguridad. Si bien es conveniente poner en práctica medidas de seguridad apropiadas, aplicar esta política es mucho más conveniente que dejar que los usuarios sigan pensando erróneamente que se les está suministrando algún tipo de seguridad. No obstante, si se suministra servicio de cifrado o cualquier otro tipo de servicio en la red, la política tendrá que cambiarse para reflejar dicho hecho. La política puede ser seguida por una declaración donde se establezca que es responsabilidad del usuario suministrar tanto el cifrado como cualquier otro tipo de medida de seguridad que requiera su información.

Políticas Relacionadas: “[Protección de la Información](#)” y “[Responsabilidades de Terceros en la Seguridad Informática](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

13. Direcciones Internas de la Red

Política: Las direcciones de los sistemas internos, las configuraciones y la información relacionada con el diseño de sistemas para los sistemas conectados en red de la Empresa X, deben ser restringidas de tal manera

que tanto los sistemas como los usuarios que no pertenezcan a la red interna de la Empresa X no puedan acceder a dicha información.

Comentario: Esta política impide que los hackers y otros terceros no autorizados obtengan información sobre la red interna y los sistemas de la Empresa X conectados a ella. El énfasis de esta restricción es que los ataques se harán más difíciles sin el acceso fácil a esta información. Mientras mayor conocimiento tenga un atacante sobre las configuraciones internas, mayores serán las oportunidades que tendrá de entrar de manera no autorizada. Si existen muchos cortafuegos, la información sobre las direcciones de los correos electrónicos internos es compartida con máquinas externas a la red, develando en forma inadvertida un blanco para posibles ataques futuros. Varios cortafuegos suministran la traducción de las direcciones de las redes como forma de incrementar la seguridad. Cuando se utilizan estos servicios de traducción, las direcciones de correos electrónicos compartidas con externos son diferentes a las direcciones utilizadas en las redes internas. La política está respaldada por esta característica del cortafuego. Esta política exige además que los administradores responsables de los cortafuegos establezcan restricciones al control de acceso de tal manera que comandos como PING no puedan ser utilizados por entes externos para recopilar información de las máquinas conectadas a la red interna. Esta política supone que la Empresa X utiliza conexiones con redes externas.

Related Topic: “[Entrega de Documentación de Sistemas](#)” y “[Liberación de Información de la Organización](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

14. Dominios en la Red

Política: Todas las grandes redes que atraviesan límites nacionales u organizacionales deben tener dominios lógicos definidos por separado, cada uno protegido con perímetros adecuados de seguridad y mecanismos de control de acceso.

Comentario: Esta política requiere que el personal de administración de redes revise los controles de acceso de las redes grandes, tales como las redes de área amplia. Si bien cada dominio lógico no necesita un mecanismo de control de acceso individual, esta decisión debe ser justificada por la gerencia. A menudo las redes grandes permiten que los usuarios las utilicen a

sus anchas sin interrupción alguna. Muchos diseñadores de sistemas de redes escogen el enfoque de la "no restricción", ya que resulta más fácil implantar y mantener una red de este tipo. Los dominios lógicos a los que hace referencia esta política pueden ser unidades organizacionales, actividades o localidades. Las barreras pueden ser activadas a través de comunicaciones vía módulo de interface, enrutadores, puertas de enlace, cortafuegos, grupo de módems con contraseñas dinámicas y demás componentes de la red que incluyan controles de acceso. El método más utilizado para restringir el acceso a una red son las contraseñas, si bien otros mecanismos tales como el cifrado también pueden ser utilizados.

Políticas Relacionadas: "[Conexiones Discadas](#)", "[Diseminación de la Información](#)," e "[Identificación Positiva para Uso del Sistema](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

15. Sistemas de Detección de Intrusos

Política: Todos los computadores multiusuario conectados a Internet deben tener activo un sistema de detección de intrusiones autorizado por el departamento de Seguridad Informática.

Comentario: Esta política garantiza que aquellos sistemas conectables a Internet estarán protegidos por herramientas automatizadas que inmediatamente detectan ataques, sean positivos o negativos. Un sistema de detección de intrusiones (IDS, por sus siglas en inglés), controla la actividad del usuario y la compara con una base de datos que contiene métodos de ataque conocidos. De existir una coincidencia con la base de datos, el IDS notificará inmediatamente a los administradores de sistemas, lo que permite que haya una respuesta inmediata, como aislar un sistema de una red interna o desactivar algunos identificadores de usuario. Existen alternativas más económicas pero que no notifican inmediatamente, pero sí informan sobre los cambios que realiza el atacante. Depende del departamento de Seguridad Informática decidir cuál herramienta resultará más apropiada para la organización que acoja esta política. El alcance de la política podría ser ampliado si la palabra "multiusuario" fuera eliminada, lo que resultaría en la inclusión de los computadores personales y las estaciones de trabajo dentro del alcance de esta política.

Políticas Relacionadas: "[Revisión de Registros del Sistema](#)" y "[Registro de Inhabilitaciones](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

16. Sistemas de Detección de Intrusos Basados en Servidor

Política: Un sistema de detección de intrusiones (IDS, por sus siglas en inglés) basado en servidor y con autorización del departamento de Seguridad Informática, debe estar activo en todos los servidores de correo, los servidores Web, los servidores de las aplicaciones, los servidores de las bases de datos y los cortafuegos conectados a cualesquiera redes externas.

Comentario: Esta política especifica qué tipos de máquinas deben poseer un sistema de detección de intrusiones (IDS), con la debida autorización del departamento de Seguridad Informática. La política hace referencia a un IDS basado en servidor, si bien existe otro tipo denominado IDS basado en red. Un IDS basado en red es un computador dedicado que se ubica junto al cortafuego, pero las decisiones en cuanto a la ubicación y despliegue del IDS basado en red son responsabilidad de los especialistas en redes de Tecnología Informática. Esta política recuerda a los administradores la vulnerabilidad de sus sistemas a ataques y que es esencial tener un IDS en sus sistemas.

Políticas Relacionadas: "[Registros Espejos Remotos](#)" y "[Revisión de Registros del Sistema](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Cortafuegos de Computadores Personales y Estaciones de Trabajo

Política: Todos los computadores personales y estaciones de trabajo con acceso a Internet mediante discado, por línea de suscripción digital, por red digital de servicios integrados, por módem por cable o por conexiones similares, deben tener sus propios cortafuegos instalados y continuamente activos.

Comentario: Esta política protege los computadores personales conectados directamente a un proveedor de servicios de Internet y no a un cortafuego de la empresa. Si bien los cortafuegos no eran considerados una necesidad en los computadores personales, hoy día es una práctica recomendada. Los hackers, los espías industriales, los delincuentes y demás atacantes, utilizan software de identificación de vulnerabilidades para explorar la Internet e identificar las máquinas a atacar.

Si un computador personal no está protegido con un cortafuego, podría ser accesible a terceros a través de Internet.

Políticas Relacionadas: “Acceso a Internet Sin Cortafuegos” y “Conexiones Discadas”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

18. Acceso del Administrador al Cortafuego de Internet

Política: Todos los cortafuegos de la Empresa X conectados a Internet deben tener un canal de acceso adicional, el cual permita que un administrador autorizado pueda conectarse en medio de un ataque de negación de servicio.

Comentario: Esta política garantiza que los administradores podrán tener acceso privilegiado a los cortafuegos en medio de un ataque de negación de servicio. De tener sólo privilegios de acceso a Internet, el ataque puede impedir su conexión. Si quedan por fuera, se les hará mucho más difícil manejar el ataque ya en proceso. Esto podría ser especialmente problemático si los administradores se encuentran a cierta distancia del cortafuego, o necesitan conectarse durante la noche desde sus hogares u otra ubicación que no sea el sitio de trabajo. Si se usan líneas de discado para acceder a los canales adicionales, es importante utilizar técnicas extendidas de autenticación de usuario, por ejemplo, contraseñas dinámicas o biométricas, y no sólo las contraseñas fijas tradicionales.

Políticas Relacionadas: “Cortafuegos de Servidores Web” e “Inhabilitación de Componentes Críticos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

19. Cortafuegos de Servidores Comerciales de Internet

Política: Todos los servidores comerciales Internet, inclusive los servidores de pagos, servidores de bases de datos y servidores Web, deben estar protegidos por cortafuegos en una zona desmilitarizada.

Comentario: Esta política protege a los servidores comerciales Internet tanto de los usuarios de Internet como de los usuarios de una red interna. En esta

actividad, es común el uso de cortafuegos y la arquitectura es denominada generalmente zona desmilitarizada (DMZ, por sus siglas en inglés). En aplicaciones tales como las que se utilizan para navegar en la web, los cortafuegos se pueden utilizar para limitar las interacciones con los servidores comerciales. Estas limitaciones reducen las probabilidades de que los hackers y demás personas no autorizadas pongan en peligro estos servidores comerciales de Internet. El uso de una DMZ no impide la transmisión autorizada de información a través de una DMZ. Esta política utiliza el concepto de aislamiento para ayudar a proteger los sistemas informáticos.

Políticas Relacionadas: “Cortafuegos de Servidores Web”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

20. Servidores Públicos en Internet

Política: Los servidores públicos en Internet se deben ubicar en subredes, aparte de las redes internas de la Empresa X, y a las cuales se haya restringido el paso del público mediante enruteadores o cortafuegos.

Comentario: Esta política garantiza que los instaladores y administradores de sistemas no instalarán servidores públicos de Internet en las mismas redes que las intranets. Si no se utiliza una subred con controles de flujo, el público en general podrá acceder a los computadores internos y aumentará la posibilidad de que personas no autorizadas accedan a información sensible. Esta política resulta adecuada para una organización con muchos sitios web, con diferentes grados de sensibilidad que puedan requerir el uso de cortafuegos.

Políticas Relacionadas: “Cortafuegos de Servidores Comerciales de Internet” y “Almacenamiento en Servidores Web y Comerciales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

21. Conexiones Discadas

Política: Todas las líneas discadas entrantes, con conexión a las redes internas o a los sistemas informáticos de la Empresa X, deben pasar por un punto de control adicional con la autorización del departamento de Seguridad Informática.

Comentario: Esta política restringe las conexiones discadas de terceros, tales como clientes, vendedores, ejecutivos en viajes de negocios y técnicos que trabajan desde sus hogares. No se recomienda que estos usuarios de discado se puedan conectar directamente con los sistemas de escritorio en las oficinas y probablemente acceder a las redes internas. Esta política requiere que todas las llamadas pasen a través de un punto de acceso central que el departamento de Seguridad Informática haya calificado como seguro. A este nivel, como alternativa a solicitar dos niveles de contraseñas, algunas organizaciones pueden activar sistemas de autenticación extendida de usuarios. La ventaja de utilizar técnicas de autenticación extendida de usuarios, es que los usuarios no tienen que conectarse dos veces. Este enfoque es consistente con el inicio de sesión único y se podría añadir una frase a la política donde se explique esta opción. Los cortafuegos son la vía más común para mantener a los hackers y demás invasores alejados de los sistemas de una organización. Esta política es en parte una forma de reconocer que las contraseñas fijas tradicionales no proporcionan suficiente seguridad. El alcance de esta política se puede restringir a las máquinas multiusuario, lo que excluiría a los sistemas de escritorio. No se recomienda este tipo de modificación, pero puede resultar necesario en algunos ambientes. Esta política se puede redactar de manera tal que exija el aislamiento de todos los sistemas de discado directo, y así evitar cualquier tipo de conexión con las redes internas u otras máquinas multiusuario. Este tipo de conexión se puede utilizar para la realización de pruebas así como para otros fines, pero sólo si no se exponen otros sistemas. Si bien en esta política se incluyen todos los tipos de conexiones discadas, la misma se podría redactar para reducir su alcance a llamadas entrantes. Si bien se atienden las vulnerabilidades mayores, este alcance limitado de la política haría la carga más llevadera para los usuarios.

Políticas Relacionadas: “[Sistemas Que Aceptan Llamadas Discadas Entrantes](#),” “[Acceso Remoto de Terceros](#),” “[Conexiones de Discado Directo](#),” “[Modem de Estaciones de Trabajo](#),” y “[Aislamiento de Sistemas con Información Secreta](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

22. Conexiones a Redes Externas en Tiempo Real

Política: Todas las conexiones entrantes en tiempo real a las redes internas de la Empresa X o a sistemas de computación multiusuario, deben pasar por un punto adicional de control de acceso.

Comentario: Esta política garantiza que los límites de una red interna siempre cuentan con mecanismos confiables de control de acceso. Si las fronteras de la red no pueden ser protegidas, significa que los controles dentro de la misma son inútiles. Un cortafuego es una máquina dedicada en la cual no se pueden ejecutar aplicaciones, dado que su única función es la de controlar los accesos. Esto hace posible eliminar el software no útil para los sistemas. La ausencia de estas rutinas disminuye la probabilidad de poner en peligro el sistema. Esta política exige que todas las conexiones externas en tiempo real posean un cortafuego u otro sistema de seguridad parecido. Dado que el correo electrónico, el suministro de noticias y otros servicios de red de almacenamiento y reenvío no se realizan en tiempo real, no tienen necesidad de un cortafuego. El uso de máquinas individuales como cortafuegos, indican la probabilidad que tiene el personal administrativo responsable de los sistemas de seguridad, de cometer fallas en los sistemas de control de acceso a los computadores internos, sin permitir una entrada masiva a la red de la organización. Esta política tiene un alcance que va más allá de la Internet. Por ejemplo, se puede aplicar igualmente a las redes con valor agregado y a las líneas discadas.

Políticas Relacionadas: “[Identificación Positiva para Uso del Sistema](#)” y “[Control de Acceso a Computadores de Red](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

23. Configuración de Cortafuegos

Política: Todos los cortafuegos de la Empresa X que estén conectados a Internet se deben configurar de tal manera que todo servicio predeterminado en Internet se desactive, permitiendo sólo aquellos servicios autorizados por escrito por el departamento de Seguridad Informática.

Comentario: Esta política impide a los administradores de sistemas suministrar un tipo de servicio al cliente que pueda comprometer la seguridad de los sistemas. Dichos administradores, o los responsables del manejo de los cortafuegos, deben estar autorizados para proveer

cualquier nuevo servicio. Algunos servicios se consideran de alto riesgo si no se toman medidas de control adicionales. Se puede generar un ambiente informático caótico y difícil de proteger, si se permite el uso de todos los servicios predeterminados a través de un cortafuego. Esta política no se aplica a los cortafuegos de la intranet.

Políticas Relacionadas: “Mal Funcionamiento del Control de Acceso” y “Diseminación de la Información”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

24. Computadores para Cortafuegos

Política: Todos los cortafuegos utilizados para proteger la red interna de la Empresa X, se deben ejecutar en computadores individuales y sin funciones adicionales.

Comentario: Esta política aumenta la seguridad de los cortafuegos desplegados al disminuir las posibilidades de ser puestos en peligro por los hackers. Esta política utiliza la simplicidad para garantizar que los cortafuegos no serán rechazados a favor de otras aplicaciones ejecutadas en la misma máquina. Utilizar los cortafuegos para otros objetivos implica la creación de nuevas vías de ataques para los intrusos. Por ejemplo, de actuar el cortafuego como servidor de correo, puede correr peligro por una falla del software para correo. Se recomienda la utilización de un cortafuego dedicado, ya que éstos se han diseñado con objetivos diferentes a los de otras máquinas. Tener una máquina dedicada garantiza que aquel software que resulte innecesario, tales como los compiladores, se podrán eliminar sin poner en peligro la funcionalidad del cortafuego. El precio relativamente bajo del hardware hace que la aplicación de esta política sea factible y una buena práctica.

Políticas Relacionadas: “Remoción de Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

25. Cambios a Configuración de Cortafuegos

Política: No se deben cambiar las reglas para configurar cortafuegos, así como las reglas permitidas para el suministro de servicios, sin la previa autorización del departamento de Seguridad Informática.

Comentario: Esta política impide cambios no autorizados a las reglas de los cortafuegos que puedan comprometer la seguridad de la red interna de una organización. Por ejemplo, puede que un administrador del sistema esté atendiendo la queja de un usuario e inicia un nuevo servicio a través del cortafuego. Como resultado, pudiera también estar exponiendo la red interna a la intrusión de un hacker. Esta política establece reglas para la configuración de cortafuegos y para el suministro de servicios como relativamente fijas, no para ser cambiadas individualmente por un administrador a su gusto. Dado que los cortafuegos son el punto de entrada a una red interna, su configuración y los servicios admisibles deben estar estrictamente controlados. Debido a que en muchas organizaciones el departamento de Seguridad Informática no administra los cortafuegos directamente, esta política mantiene cierto control en el Departamento de Seguridad Informática, en lugar de transferirlo a los administradores del sistema.

Políticas Relacionadas: “Computadores para Cortafuegos” y “Acceso a Internet”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

26. Conexiones a Internet

Política: Todas las conexiones entre las redes internas de la Empresa X e Internet o cualquier otra red de computación públicamente accesible, deben incluir un cortafuego autorizado y los controles de acceso correspondientes.

Comentario: Esta política tiene la intención de impedir que los departamentos, las divisiones y demás unidades organizacionales se conecten directamente a Internet o cualquier otra red de computación externa. Algunas organizaciones no tienen una autoridad central que controle la seguridad de la red a lo largo de la organización. Como resultado, se ha convertido en práctica común que las unidades organizacionales establezcan sus propias conexiones a Internet. Esta política define una vía obligatoria para realizar las conexiones. La consistencia en los controles de acceso a la red es absolutamente necesaria para contar con una seguridad eficaz. Estas conexiones pueden ser utilizadas a futuro por personas ajenas con el fin de acceder a las redes internas de manera no autorizada. Esta política se puede ampliar con una frase aclaratoria sobre la admisibilidad de las conexiones discadas desde un computador personal independiente.

Políticas Relacionadas: “Acceso Entrante a Internet,” “Acceso Remoto de Terceros,” “Dominios en la Red,” “Mecanismo Unico de Acceso,” “Modem de Estaciones de Trabajo,” y “Aislamiento de Sistemas con Información Secreta”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

27. Sistemas de Directorios Compartidos

Política: El uso de sistemas de directorios compartidos en cualquier computador de la Empresa X conectado con Internet o accesible desde Internet, debe estar autorizado por la gerencia de Seguridad Informática.

Comentario: Esta política reduce el daño que los hackers o demás invasores pueden ocasionar si comprometen la seguridad de un computador de fácil acceso a través de Internet. Si se utiliza un sistema de directorio compartido, entonces el trabajo de los invasores se facilita enormemente. De no contar con un sistema de directorio compartido, los invasores deben acceder a las máquinas individualmente. Dentro de esta política se asume que las contraseñas fijas u otros controles de acceso difieren de una máquina a otra. Si todas son iguales, la función de esta política es la de aumentar el trabajo de los administradores del sistema. La política tiene que ver solamente con los identificadores de usuario de uso general, y no con los usuarios anónimos o a los formatos automáticos que limitan las actividades de un usuario en Internet. Esta política limita los lugares de la red donde se pueden utilizar los sistemas de inicio de sesión único, aunque los usuarios los prefieran porque ahorran tiempo y esfuerzo.

Políticas Relacionadas: “Autorización para Conexiones a Internet” y “Relaciones de Confianza entre Servidores”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

28. Conexiones en Red con Organizaciones Externas

Política: La creación de una conexión directa entre los sistemas de la Empresa X y los computadores de organizaciones externas a través de Internet o cualquier otra red pública, debe estar autorizada por el gerente de Seguridad Informática.

Comentario: Los cortafuegos conectados a Internet pueden definir un canal protegido que permite a los individuos de una organización navegar a través de Internet y acceder en forma segura a los computadores de otra organización. Si bien esto resulta útil en algunas circunstancias, como en un proyecto conjunto, también implica riesgos adicionales de seguridad. Antes de establecer tales conexiones, esta política requiere que los usuarios estén autorizados por la gerencia de Seguridad Informática o por el ente responsable de la seguridad de la información. Antes de autorizar tales conexiones, el gerente de Seguridad Informática debe precisar quién podrá tener acceso a los sistemas de la Empresa X, qué información sobre los sistemas de la Empresa X estarán disponibles, qué sistemas de registro darán seguimiento a la actividad y qué necesidades de negocios existen en relación con esta conexión. El departamento de Seguridad Informática puede tomar en cuenta otra vía para lograr la productividad requerida sin introducir vulnerabilidades adicionales en seguridad informática.

Políticas Relacionadas: “Acceso Remoto de Terceros,” “Dominios en la Red,” “Mecanismo Unico de Acceso,” “Modem de Estaciones de Trabajo,” y “Aislamiento de Sistemas con Información Secreta”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

29. Cambios en la Línea de Comunicación

Política: Los trabajadores y los proveedores no deben hacer ningún tipo de arreglos o completar la instalación de líneas de voz o datos con ninguna compañía telefónica, si no han obtenido la autorización del director del departamento de Telecomunicaciones.

Comentario: Esta política garantiza que sólo se instalarán en las líneas de comunicación las modificaciones previamente autorizadas. Establecer comunicaciones no autorizadas puede comprometer la seguridad de los sistemas de la Empresa X. Las líneas no autorizadas suministran vías de ataque a los hackers si no han sido aseguradas adecuadamente. La política garantiza que todas las líneas cumplen los requerimientos existentes sobre controles de acceso. Esta política es importante para los computadores personales y las estaciones de trabajo, muchos de los cuales están conectados con módems no autorizados. Si no hay seguridad adicional para estos sistemas, cualquiera se puede conectar a ellos utilizando un conmutador de la red telefónica pública y acceder a una conexión de red interna. Algunas organizaciones pueden expandir el

alcance de la política para hacer mención específica de tales dispositivos módem. Al igual que otros aspectos relativos a seguridad computacional y comunicacional, hay cosas que deben hacerse de manera centralizada; por ejemplo, establecer vías de comunicación y desarrollar políticas de seguridad. Las palabras de esta política que hacen referencia a la autorización del departamento de Telecomunicaciones se pueden reemplazar por autorización del departamento de Seguridad Informática.

Políticas Relacionadas: “[Implantación de Sistemas Multiusuario](#),” “[Interconexión de Sistemas](#),” y “[Modem de Estaciones de Trabajo](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

30. Configuración de Conexiones a la Red

Política: Todas las redes internas deben estar configuradas de tal manera que prevengan o detecten los intentos de conexión de computadores no autorizados.

Comentario: Esta política impide a los intrusos conectar computadores no autorizados a una red interna. Aun cuando un intruso acceda inmediatamente a un computador interno autorizado, el hecho de que una máquina no autorizada esté conectada a la red interna permite al intruso realizar varios ataques. Estos ataques incluyen reemplazar un protocolo en Internet y desactivar la intercepción de contraseñas a través de un rastreador de paquetes. Esta política exige el uso de concentradores seguros, comunicaciones intranet cifradas o tecnologías similares que impidan el acceso de máquinas no autorizadas a la red, o por lo menos que detecten su presencia. La detección de un computador no autorizado en una red interna pueda alimentar un sistema de detección de intrusiones, una red o un sistema de manejo de sistemas y obtener una respuesta del personal técnico, tal como un equipo de respuesta ante emergencias informáticas. El uso de una política como ésta también garantiza que se respetarán las normas de computadores de escritorio. Una vez que un computador de escritorio nuevo haya demostrado ser consistente con las normas internas, se le asignará una dirección interna a la máquina que le permita acceder a la red interna.

Políticas Relacionadas: “[Puertos de Red en Oficinas Vacías](#)” y “[Conexiones Personales a la Red](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

31. Criterios de Seguridad para Conexión a Intranet

Política: Todos los sistemas informáticos y segmentos de redes deben satisfacer todos los criterios de seguridad establecidos por la gerencia de Seguridad Informática incluyendo, sin limitaciones, tener un cortafuego aceptable, un sistema aceptable de autenticación de usuario, un sistema aceptable de control de privilegios de usuario, un proceso establecido de control de cambios, una definición clara y por escrito de las responsabilidades sobre el manejo de sistemas y una documentación operacional adecuada, antes de ser conectados a la intranet de la Empresa X.

Comentario: Esta política establece la intención de la gerencia de impedir que los sistemas manejados localmente se conecten a la intranet sin cumplir los controles de seguridad adecuados. Permitir conexiones ilimitadas a los servidores de intranet y a los segmentos de red, compromete a las demás máquinas en la Internet. Estar conectado a Internet es deseable desde un punto de vista corporativo, y esta política apalanca el deseo de que los sistemas manejados remotamente cumplan algunas medidas básicas de seguridad. La política especifica algunas de estas medidas básicas de seguridad, pero se deben añadir otras de acuerdo con las necesidades de la organización. La política es una forma indirecta de re establecer un control centralizado a lo largo de la organización sobre Seguridad Informática.

Políticas Relacionadas: “[Conexiones a Redes de Terceros](#)” y “[Autorización para Conexiones a Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

32. Inventario de Conexiones a Redes Externas

Política: El departamento de Seguridad Informática debe mantener un inventario actualizado de todas las conexiones a las redes externas incluyendo, sin limitantes, redes telefónicas, redes EDI, extranet e Internet.

Comentario: Esta política ofrece al departamento de Seguridad Informática una lista completa de todos los puntos de acceso a las redes internas. Si bien los hackers se introducen a través de las redes, es necesario que el departamento de Seguridad Informática tenga conocimiento de todos los puntos de acceso externo. El personal del departamento de Seguridad Informática centra su atención en estos puntos de acceso para garantizar que los controles, tales como los cortafuegos

y los enrutadores, están establecidos y funcionando. Atención especial debe prestarse al acceso de los socios a la red de una organización, lo que también estaría incluido en esta política. Desde un punto de vista generalizado, esta política requiere que el departamento de Seguridad Informática enfoque su atención en un área específica. Muchas organizaciones no tienen conocimiento de todos los puntos de acceso hacia sus redes, lo que hace que cuando ocurre una intrusión experimenten serias dificultades tratando de aislar el punto de entrada utilizado por los hackers, los espías industriales y demás intrusos.

Políticas Relacionadas: “[Inventario de Activos — Tecnología](#)” e “[Inventario de Activos — Información](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

33. Provisión de Servicios de Redes Públicas

Política: Antes de utilizar las redes públicas para suministrar servicios de red a los subscriptores, el departamento legal de la Empresa X debe evaluar el alcance y la naturaleza de las responsabilidades existentes, y la alta gerencia debe aceptar tácitamente estos riesgos.

Comentario: Comprometerse para brindar servicio de re-envío de mensajes en Internet, como autoridad de certificación, como centro notarial de claves de cifrado, como punto de distribución de claves de cifrado u otro proveedor de información, puede exponer a la Empresa X a riesgos no considerados con antelación. La Empresa X puede ser considerada responsable de fraudes cometidos con sus sistemas, o si éstos han sido utilizados por delincuentes para almacenar datos de tarjetas de crédito robadas. Esta política impide que el personal de la Empresa X ofrezca las instalaciones de la misma hasta que los riesgos y demás responsabilidades hayan sido identificados plenamente y aceptados por la alta gerencia.

Políticas Relacionadas: “[Sin Responsabilidad en Mensajes](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

34. Números de Acceso a Computadores

Política: La información relacionada con el acceso a los sistemas de computación y comunicacionales de la Empresa X, tales como números telefónicos de discado

por módem, se considera confidencial y no debe ser publicada en la Internet, en directorios telefónicos, en tarjetas de presentación comercial o puestas a disposición de terceros, sin la autorización previa por escrito del director del departamento de Sistemas Informáticos.

Comentario: Esta política impide que la información sobre el acceso al sistema pase a manos de terceros no autorizados, quienes podrían utilizar esta información para entrar ilegalmente a los sistemas de la Empresa X. Los hackers pueden identificar esta información a través de recursos disponibles públicamente, acción que debe ser obstaculizada por las organizaciones al no publicar este tipo de información. Las organizaciones proclives a la seguridad podrían desear la ampliación del alcance de esta política con el propósito de incluir identificadores de usuario y otros medios de identificación similares, aunque esto dificulta las comunicaciones inter-organizacionales. Para estas organizaciones, puede resultar apropiado prohibir la impresión de dicha información en tarjetas de presentación, y por otro lado permitir que los responsables la difundan según el caso. No obstante, se pueden hacer excepciones documentadas para la mayoría de las organizaciones.

Políticas Relacionadas: “[Guías Telefónicas Internas](#),” “[Divulgación de los Controles del Sistema Informático](#),” “[Números de Cuenta Bancaria](#),” e “[Información en Mensaje de Inicio de Sesión](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

35. Cambio de Números Discados

Política: Los números telefónicos de las comunicaciones de computación de la Empresa X deben ser cambiados por lo menos una vez al año.

Comentario: La intención de esta política es impedir que los hackers u otros entes no autorizados ubiquen los números telefónicos que comunican a los computadores de la Empresa X. Los hackers intercambian a menudo esa información, lo que significa que con el tiempo un número mayor de individuos conocerán los detalles sobre el acceso a los sistemas de las organizaciones. Cambiar periódicamente los números de acceso telefónico puede considerarse como cambiar las contraseñas y las claves de cifrado. Por lo menos logrará interrumpir muchos accesos no autorizados que hasta los momentos pasaban desapercibidos. Muchas veces, además de los hackers y de los espías industriales, los ex-empleados pueden llevar a cabo usos inapropiados

también. El marco de tiempo mencionado en la política puede ser modificado sin alterar de manera significativa el impacto de la política. Muchas organizaciones pueden considerar que esta política entorpece sus operaciones habituales, por lo cual una evaluación del tiempo y esfuerzo requeridos para realizar ajustes en los números telefónicos debe ser llevada a cabo antes de adoptar la política. Algunas organizaciones consideran que cambiar los números telefónicos tiene consecuencias negativas en las relaciones con los clientes y usuarios, y por lo tanto no aprueban esta política. Hay otras formas de compensar el hecho de no cambiar los números telefónicos, por ejemplo a través del uso de contraseñas dinámicas.

Políticas Relacionadas: “[Documentación de Cambios en Sistemas de Producción](#)” y “[Cambios Obligatorios de Contraseña](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

36. Conexiones Salientes

Política: Todos los usuarios que hayan establecido conexiones salientes desde las oficinas de la Empresa X, deben tener autenticadas sus identidades antes de establecer estas llamadas y deben utilizar el grupo de módem dedicado para tal fin.

Comentario: Esta política impide que los hackers y demás entes no autorizados establezcan conexiones a través de múltiples computadores en diferentes redes, con la intención de frustrar los intentos de rastreo de llamadas o del registro de su actividad. Los hackers, los espías industriales y otros usuarios no autorizados están utilizando esta técnica para ocultar sus actividades. Esta política garantiza que los hackers no podrán discar hacia afuera una vez entran en el sistema de la Empresa X. Esta política permitirá a la organización decidir sobre quién quedará autorizado para establecer conexiones salientes. Cualquier proceso de restricción de accesos será ineficiente si no cuenta con un mecanismo de control de accesos con un grupo de módem. Se pueden utilizar restricciones en cuanto a quién puede discar hacia afuera para disminuir las probabilidades de que los trabajadores internos envíen información confidencial o propiedad de la empresa a través de una conexión de discado, asumiendo que no tienen acceso a Internet. La política respalda el uso de un sistema de reversión de cargos que asigna los costos de llamadas de larga distancia a ciertos departamentos, individuos o proyectos. La norma es autenticar sólo a los usuarios que llaman a la empresa, pero esta política puede

brindar un nivel adicional de protección. Dentro de la política, se pueden conceder excepciones a los salones de conferencia o áreas de recepción, donde los visitantes con computadores portátiles pueden establecer conexiones de salida o donde se puedan suministrar puertos de red telefónica pública analógica. Esta excepción no pondrá por ningún motivo en peligro la seguridad suministrada por la política ya que estos computadores portátiles no están conectados a las redes internas de la manera en que están conectadas las unidades de escritorio de los empleados. Esta política es imprecisa en forma deliberada en cuanto a las formas de autenticar definitivamente a los usuarios, lo que a menudo requiere que el departamento de Seguridad Informática defina con exactitud el significado de dichas palabras. La tecnología que respalda la autenticación definitiva puede variar en el tiempo sin que exista la necesidad de redactar nuevamente la política.

Políticas Relacionadas: “[Acceso Remoto de Terceros](#)” y “[Autenticación de Usuario Que Accede Vía Teléfonica](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

37. Modem por Cable

Política: No debe ser utilizado ningún módem por cable para las comunicaciones comerciales de la Empresa X, a menos que los computadores utilicen un cortafuego o una red privada virtual.

Comentario: Los módem por cable proporcionan una alternativa rápida a las líneas de discado, pero también presentan una deficiencia en cuanto a seguridad, ya que permiten que los usuarios de las subredes locales exploren las actividades de otros usuarios. Esto puede generar la divulgación de datos a través de la conexión del módem. Si se utilizan un cortafuego y una red privada virtual (VPN, por sus siglas en inglés), se pueden lograr ciertas ventajas en cuanto a rapidez con el uso de módem por cable. No se han identificado problemas similares en las líneas digitales de abonado, o en la Red Digital de Servicios Integrados, aunque se recomienda igualmente el uso de un cortafuego y de una red privada virtual para estas tecnologías. Estas tecnologías pueden resultar útiles para los teletrabajadores cuando se conectan a un computador a través de Internet.

Políticas Relacionadas: “[Cortafuegos de Computadores Personales y Estaciones de Trabajo](#)” y “[Autenticación de Usuario Que Accede Vía Teléfonica](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

38. Configuración de Modem para Llamadas Discadas Entrantes

Política: Los módem de acceso telefónico de la Empresa X no deben responder llamadas entrantes hasta el cuarto repique.

Comentario: Esta política impide la divulgación de los números telefónicos del módem a personas que deseen obtener acceso no autorizado. Esta política aplica un pequeño retardo a los que realizan llamadas hacia la empresa, y también mantiene estas líneas fuera de la lista de líneas de módem que circulan en la comunidad de los hackers. Los programas de discado automatizado realizan búsquedas de números telefónicos con conexiones a módem de computadores y, al no obtener respuesta después de algunos repiques, discan otro número.

Políticas Relacionadas: “[Estructura de las Contraseñas](#)” e “[Intentos de Contraseñas por Discado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

39. Contraseñas para Conexión Telnet

Política: Los usuarios no deben implantar conexiones Telnet en los computadores de la Empresa X utilizando contraseñas fijas tradicionales en Internet, a menos que dichas conexiones se establezcan utilizando contraseñas dinámicas u otro tipo de tecnología autorizada para la autenticación extendida del usuario.

Comentario: Esta política impide que las contraseñas fijas sean interceptadas en Internet y repetidas más tarde con el objetivo de acceder en forma no autorizada a los sistemas de la Empresa X. Con dispositivos de vigilancia apropiados y fácilmente accesibles, es muy sencillo para los intrusos capturar automáticamente las contraseñas que se mueven a través de Internet. Estos ataques pueden ser frustrados con sistemas de contraseñas dinámicas y otras técnicas de autenticación extendida de usuario, tales como huellas de voces y patrones mecanográficos del usuario. Otro objetivo de esta política es notificar al personal técnico sobre los privilegios que se permiten a través de un cortafuego u otro dispositivo de conexión a Internet.

Políticas Relacionadas: “[Acceso Entrante a Internet](#)” y “[Autentificación de Usuario Que Accede Vía Teléfonica](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

40. Filtrado de Contenido Activo

Política: Todos los subprogramas (applets) entrantes con contenido activo deben ser automáticamente eliminados por un cortafuego.

Comentario: Esta política impide daños a los computadores y a la información de los usuarios. Se puede considerar como daño el borrado del disco duro y otros eventos que se observan normalmente cuando un virus malicioso contamina un sistema. Se está incrementando el uso de los programas de contenido activo en Internet para eludir los controles de acceso existentes y así causar daños graves. Para evitar estos problemas, algunas organizaciones prohíben los contenidos activos entrantes aún cuando estén siendo utilizados en su intranet. Este enfoque, que involucra el filtrado del contenido entrante a nivel del cortafuego, elimina las opciones del usuario y logra un mayor nivel de seguridad que el enfoque que depende de las acciones del usuario. Puede ser que las organizaciones consideren muy estricta esta política.

Políticas Relacionadas: “[Ejecución de Programa Java](#)” e “[Inhabilitación de Java](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

41. Acceso a Internet

Política: Todos los accesos a Internet utilizando los computadores de las oficinas de la Empresa X deben ser enrutados a través del cortafuego.

Comentario: Esta política impide que los usuarios eluden de manera deliberada o no intencional los controles del cortafuego. Estos controles incluyen la capacidad de detectar virus en archivos descargados, buscar palabras claves en archivos salientes que indiquen sensibilidad, obstruir la conexión con algunos sitios web, registrar la actividad del usuario y bloquear la descarga de contenidos activos. Si los usuarios necesitan acceder a Internet a través de un proveedor de Internet, lo pueden hacer pero sin el equipo de la Empresa X. La política se restringe a los computadores

instalados en las oficinas de la Empresa X, debido a que los teletrabajadores y usuarios de computadores portátiles no se pueden regir por esta política.

Políticas Relacionadas:“[Acceso a Internet Sin Cortafuegos](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

42. Conexiones Directas a Internet

Política: Los sistemas informáticos internos de producción no deben estar conectados directamente a Internet, sino que deben estar conectados a un servidor comercial, a un servidor de base de datos, u otro computador intermedio dedicado a la actividad comercial de Internet.

Comentario: Esta política disminuye el daño que un hacker pueda ocasionar si se introduce en un computador de la Empresa X a través de Internet. Hoy en día algunas empresas están conectando sus sistemas de producción directamente a Internet, pero esta práctica no es muy recomendada porque, si la máquina estuviera en peligro, todos los datos de producción de esa máquina estarían bajo riesgo. Si un hacker dañara la máquina en uso, se pararía toda la actividad productiva que normalmente procesa dicho sistema. Esta política refleja una buena práctica del comercio en Internet, y dado el bajo costo de los computadores, esto no representa una fuerte carga financiera para la organización que está por adoptar esta política. Con el objetivo de ser más efectiva, la política podría incluir un sistema operativo separado u otros mecanismos de control de acceso diferentes a los del computador destinado a producción.

Políticas Relacionadas:“[Conexiones en Red con Organizaciones Externas](#)” y “[Acuerdos de Negocios por Internet](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

43. Directorios Modificables por el Público

Política: Todos los directorios modificables públicamente presentes en los computadores conectados a Internet de la Empresa X deben ser revisados y borrados todas las noches.

Comentario: Esta política impide que los computadores de la Empresa X sean utilizados como punto de arranque de información ilegal, inmoral, abusiva o personal. Existen varios casos en los que los hackers han utilizado directorios modificados públicamente en máquinas conectadas a Internet para almacenar los tipos de información que menciona esta política. Esta política también es recomendable ya que impide que la Empresa X de manera no intencionada sea declarada cómplice de un delito o el proveedor de un sistema informático controversial y visible. Los procedimientos que respaldan esta política pueden ser automatizados a través de comandos, por lo que la puesta en práctica de esta política no debe ser costosa.

Políticas Relacionadas:“[Uso Distinto al Empresarial de la Información de la Organización](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

44. Redes Inalámbricas

Política: Las redes inalámbricas utilizadas en las trasmisiones de la Empresa X deben estar configuradas para emplear cifrado.

Comentario: Esta política impide que hackers, espías industriales, ex-empleados descontentos y otros adversarios intercepten las trasmisiones inalámbricas de la Empresa X. Sin el cifrado correspondiente, estos adversarios pudieran intervenir la línea pasivamente y hasta llegar a tener acceso a las contraseñas fijas, las direcciones de las máquinas y demás información que sería utilizada para atacar los sistemas de la Empresa X. Las redes inalámbricas permiten que los adversarios ataquen los sistemas de la Empresa X desde sitios remotos. Esta política implica que el cifrado debe estar incluido en las trasmisiones vía microondas de alta velocidad, que en muchos casos no han sido cifradas tradicionalmente.

Políticas Relacionadas:“[Teléfonos Celulares o Inalámbricos](#)” y “[Transmisión Inalámbrica de Información Secreta](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

45. Puertas de Enlace a Redes Inalámbricas

Política: Las puertas de enlace a redes inalámbricas de la Empresa X deben estar siempre configuradas de tal manera que utilicen cortafuegos para revisar las comunicaciones con dispositivos remotos.

Comentario: Esta política está diseñada para enfrentar un ataque conocido como envenenamiento del protocolo de resolución de la dirección. Este ataque permite a un hacker u otro intruso aparentar que está manejando un dispositivo autorizado conectado a una red inalámbrica específica, así como también permite a un intruso enrutar el tráfico a través de una máquina no autorizada. Para no repetir ataques similares, se recomienda el uso de cortafuegos en todas las puertas de enlace a redes inalámbricas.

Políticas Relacionadas: “Modem por Cable” y “Filtrado de Contenido Activo”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

46. Sistemas en Interface con Redes Externas

Política: Todos los sistemas de la Empresa X que tengan conexión con redes externas deben estar ejecutando la última versión del software operativo suministrado por el fabricante.

Comentario: Esta política disminuye el éxito de los hackers y otros atacantes en su intento por utilizar los últimos métodos de ataque. Algunos administradores de sistemas pueden diferir la actualización del software de los cortafuegos y otros sistemas que empleen interfaces externas. Esta es una propuesta peligrosa en cuanto a seguridad y podrá ser impeditida con esta política. Los fabricantes no siempre publican los parches con suficiente antelación para evitar problemas mayores, pero si un método de ataque es lo suficientemente peligroso, los fabricantes publicarán los parches apenas se descubran las vulnerabilidades con el objeto de minimizar su propia responsabilidad. La existencia en Internet de software para la identificación de vulnerabilidades hace de ésta una política de mucha importancia. Este software permite que los atacantes determinen qué versión de software está utilizando un sistema en particular y sus correspondientes vulnerabilidades.

Políticas Relacionadas: “Versiones de Sistemas Operativos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

47. Medidas de Seguridad de la Red

Política: Las medidas de seguridad de las redes de los sistemas de producción de la Empresa X no deben ser compatibles con versiones anteriores.

Comentario: Esta política impide un ataque a la versión anterior, lo cual pondría en peligro el control correspondiente. Si bien la compatibilidad con las versiones anteriores es amigable para los usuarios y deseable desde el punto de vista de la interconectividad y la interoperatividad, es peligroso desde el punto de vista de la seguridad en las redes. Si un atacante puede obtener una versión actualizada del control para volver a una versión anterior del protocolo, entonces el atacante puede aprovecharse de las vulnerabilidades de la versión anterior, aun cuando estas vulnerabilidades hayan sido corregidas en la nueva versión. Es muy difícil diseñar un control que sea compatible con las versiones anteriores aunque sólo sea para mantener la funcionalidad y que al mismo tiempo impida que los atacantes exploten las vulnerabilidades de la versión anterior. Esta política reconoce esta debilidad y opta por la propuesta de mayor seguridad que es la de prohibir la compatibilidad con versiones anteriores.

Políticas Relacionadas: “Versiones de Sistemas Operativos” y “Sistemas en Interface con Redes Externas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

48. Dispositivos Críticos de Voz y Datos en Red

Política: Todos los dispositivos comerciales críticos que soportan el sistema telefónico de la Empresa X, su intranet, las redes de área local y las redes de área amplia, deben estar centralizadas en recintos dedicados con controles de acceso físico, con circuito cerrado de televisión, con sistemas de monitoreo de medio ambiente y otras medidas especificadas por el departamento de Seguridad Informática.

Comentario: Esta política niega el acceso físico a personas no autorizadas, a los dispositivos conectados en redes de voz y datos, tales como centrales telefónicas privadas, concentradores y enruteadores. Esto complicará la configuración de dispositivos para intervenir las líneas o sabotear estos sistemas. Debido a que mucha gente utiliza sistemas conectados en red, éstos consti-

tuyen un blanco preferido de los saboteadores. Esta política también revierte la tendencia de ubicar estos dispositivos a lo largo y ancho de una oficina, exponiéndolos a una variedad de riesgos como las interrupciones accidentales. Esta política puede incrementar los costos de cableado. El alcance de esta política podría ser ampliado con el fin de incluir todos los servidores y los computadores multiusuario. Dentro de la política se supone que la palabra "crítica" ha sido definida formalmente durante la planificación de contingencias.

8.06 Manejo y Seguridad de Medios de Almacenamiento

8.06.01 Manejo de Medios de Computación Removibles

1. Discos Flexibles

Política: Todos los discos flexibles utilizados en la Empresa X deben ser autorizados, formateados y emitidos únicamente por el departamento de Tecnología Informática.

Comentario: Esta política impide que los trabajadores almacenen información sensible en discos flexibles, los cuales representan los medios de almacenamiento de datos más portátiles y de más fácil remoción. En la mayoría de las organizaciones, la información sensible almacenada en un disco flexible en un computador de la empresa, probablemente será legible por un computador externo. Esta política utiliza un software personalizado para cifrado integrado con el controlador de entrada / salida del disco flexible, de tal manera que cada vez que se ejecute un comando de escritura o de lectura, se invocará automáticamente el proceso de cifrado. De esta manera, estos discos serán ilegibles en computadores externos a la organización. Si un usuario quisiera enviar información a un tercero mediante un disco flexible, sería necesaria la intervención del departamento de Tecnología Informática. El software pudiera ser cargado en su totalidad desde Internet o desde CD-ROM debido a que la capacidad de los discos flexibles es muy pequeña para la mayoría de los paquetes principales. Si se adopta esta propuesta, es recomendable contar con controles adicionales, como filtros para el contenido de los correos electrónicos salientes.

Políticas Relacionadas: "Traslado de Medios" y "Prevención del Copiado de Documentos Sensibles"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

Políticas Relacionadas: "Aseguramiento de los Sistemas de Computación o Comunicación" y "Control de Acceso Físico a la Información Sensible"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Almacenamiento de Información de Clasificación Mixta

Política: Los trabajadores de la Empresa X no deben almacenar información confidencial o secreta conjuntamente con información no sensible en discos flexibles u otro medio extraíble de almacenamiento.

Comentario: Esta política evita las confusiones en cuanto al manejo adecuado de medios extraíbles de almacenamiento de datos, tales como los discos flexibles. Debido a que los procedimientos de manejo difieren dependiendo de la clasificación de los datos, mezclar las clasificaciones de datos diferentes requeriría que los discos u otros medios de almacenamiento fueran manejados con los procedimientos más estrictos, los cuales pueden convertirse en algo innecesariamente costoso e inconveniente. Otro de los objetivos de esta política es minimizar los costos relacionados con la seguridad. Esta política fue diseñada para usuarios de computadores personales y estaciones de trabajo, aunque también puede ser aplicada los operadores de mainframes y demás operadores que manejan medios para almacenamiento de datos. En esta política se asume que la palabra "sensible" ha sido definida en otra política.

Políticas Relacionadas: "Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad," "Clasificaciones de Medios de Almacenamiento de Datos," y "Clasificación de Datos en Cuatro Categorías"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

3. Borrado de Información Sensible

Política: Cuando la información sensible de la Empresa X se borra de un disco, cinta u otro medio reutilizable de almacenamiento de datos, se debe acompañar dicha acción con una operación repetida de reescritura para eliminar la información sensible.

Comentario: Con la mayoría de los sistemas operativos, los comandos normales para borrado y copiado de un archivo de disco, eliminan su entrada de una tabla de asignación de archivos o de un directorio. Lo importante en el uso de este proceso de borrado para eliminar información sensible, es que puede programarse para que suceda automáticamente. Se puede escribir un archivo de comandos para salir de un medio de almacenamiento de datos cada vez que se elimine información sensible. Algunos sistemas operativos hacen esto automáticamente y el usuario no tiene que enterarse de este proceso. De no contar con un enfoque automatizado, los usuarios pueden invocar un software autorizado para manejar este proceso, si se trata de

información sensible. La política evita que se revele de manera no autorizada aquella información sensible que pueda quedar en los medios informáticos, bien sea que el proceso se maneje automáticamente o por usuarios finales. El enfoque automatizado se recomienda ya que no se puede contar con los usuarios de manera consistente para terminar esta tarea. Existen paquetes comerciales para realizar este proceso de sobreescritura. Esta tecnología no es pertinente para el medio de almacenamiento WORM, el cual dada su naturaleza no es reutilizable. Esta política asume que el término "sensible" está definido en otra política.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Información de Registro del Cliente,” “Enlaces Entre la Información Privada y la Identificadora,” y “Transferencia de Información Sensible”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

8.06.02 Disposición Final de los Medios

1. Destrucción de Información Sensible

Política: La destrucción de la información sensible resguardada en medios informáticos de almacenamiento, debe llevarse a cabo sólo con métodos autorizados de destrucción, incluyendo trituradores de documentos u otros equipos autorizados por el departamento de Seguridad Informática.

Comentario: Esta política sirve de guía de métodos autorizados para destruir la información confidencial que resida en los medios de almacenamiento de computación. Los mejores métodos para destruir información son la incineración, la trituración u algún otro método que inutilice los medios de almacenamiento. Otra técnica es un método de desmagnetización que utiliza campos electromagnéticos para borrar datos. La desmagnetización no es utilizable en CD-ROM, cartuchos óptico-magnéticos y otros medios de almacenamiento que no usan enfoques magnéticos tradicionales. Los programas de sobreescritura escriben secuencias repetidas de unos y ceros sobre la información, disminuyendo así las probabilidades de que la información sea recuperada. Puede requerirse asistencia técnica debido a que la sobreescritura puede que sea no aceptada por algunos medios de almacenamiento. En organizaciones con necesidades menos apremiantes en cuanto a seguridad, son aceptables los medios menos definitivos de destrucción. Esta

política está redactada para las organizaciones militares, diplomáticas y demás organizaciones con altos niveles de seguridad. Los métodos mencionados en este comentario y que no destruyen la información, permiten el reciclaje de los medios, el ahorro de dinero y la reducción de la contaminación ambiental. Esta política asume la existencia de otra política que defina el término "información sensible".

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Borrado de Información Sensible,” “Materiales para la Generación de Contraseñas,” “Materiales para la Generación de Claves,” y “Cifrado de Almacenamiento en Disco”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

2. Disposición de Información en Papel

Política: Al eliminar cualquier información secreta, confidencial o privada en forma impresa, ésta debe ser triturada o incinerada.

Comentario: Esta política evita que se ubique información en el cubo de desperdicios. Recuperar información de cubos de desperdicios es la táctica favorita de los hackers, los investigadores privados, los

espías industriales, los espías militares y la policía. En muchas jurisdicciones es un método tanto legal como exitoso para obtener información importante. Muchas organizaciones especifican el tipo de trituración obligatorio que se exige. Esta política asume la existencia de otra política que defina los términos "secreta, confidencial o privada".

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías," "Retención de Información Sensible para su Destrucción," "Destrucción de Materiales para Generación de Claves," y "Materiales Usados con Información Sensible"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Máquinas Trituradoras de Papel en Tiras

Política: Las trituradoras de papel en tiras no deben utilizarse en ninguna de las instalaciones de la Empresa X.

Comentario: Esta política garantiza que los usuarios triturarán sus documentos, y que ello les brindará suficiente seguridad. Aunque son ampliamente utilizadas, las trituradoras de papel en tiras pueden ser superadas por un adversario empeñado en reconstruir el material. El uso extendido de estas trituradoras se debe a su bajo costo. En vez de trituradoras de tiras, las organizaciones deberían utilizar trituradoras que generen papelillo o algún otro tipo de papel de pequeñas dimensiones.

Políticas Relacionadas: "Destrucción de Información Sensible" y "Manejo de Mensajes de Correo Electrónico"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

4. Contenedores Seguros de Información

Política: La información secreta debe ser destruida inmediatamente y la información sensible a eliminar debe ser colocada en un recipiente bajo llave destinado a la destrucción de material dentro de las oficinas de la Empresa X, y nunca debe ser colocada en cubos para desperdicios, cubos de reciclaje u otros sitios de acceso público.

Comentario: Esta política orienta al personal en la destrucción adecuada y la disposición final del material sensible. La información secreta debe ser destruida

inmediatamente por su alta sensibilidad. Esto disminuirá el riesgo de que alguien tenga acceso al recipiente destinado a la destrucción y extraiga el material. La política asume que las palabras "sensible" y "secreta" han sido definidas en otras políticas, como por ejemplo una política de clasificación de datos. La política también asume que están publicados los métodos autorizados para la destrucción de material.

Políticas Relacionadas: "Eliminación de la Información de Pago," "Copias Sobrantes de Información Sensible," y "Retención de Información Sensible para su Destrucción"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

5. Instrucciones para la Destrucción de la Información

Política: Todos los materiales dentro del recipiente de destrucción deben ser destruidos de acuerdo con los procedimientos autorizados, sin tomar en cuenta los detalles sobre el reciclaje.

Comentario: Los integrantes del personal de seguridad encargados de la destrucción de la información pueden estar preocupados por la ecología y pensar que no deben destruirse algunos artículos, los cuales podrían reciclarse sin ocasionar daño a la Empresa X. Esta política prohíbe tomar este tipo de decisiones. Esta política garantiza que toda la información que deba destruirse será destruida, y elimina la razón por la cual el personal de seguridad podría proceder a examinar la información a la que no tienen acceso autorizado. Esta política generalmente se distribuiría entre el personal de seguridad.

Políticas Relacionadas: "Copias Sobrantes de Información Sensible"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Procedimientos para la Destrucción de la Información Sensible

Política: Cuando ya no sea necesaria, la información sensible o valiosa de la Empresa X debe ser destruida de manera segura, utilizando los procedimientos autorizados por el departamento de Seguridad Informática.

Comentario: Esta política exige que todas las personas que manejan la información sensible de la Empresa X la eliminen de manera segura. Los procedimientos a utilizarse pueden estar especificados en unas normas establecidas o en una guía, y no en una política. Esta política asume la existencia de otra política que defina los términos "sensible o valiosa"."

Políticas Relacionadas: "Disposición de Información en Papel," "Clasificación de Datos en Cuatro Categorías" y "Destrucción de Materiales para Generación de Claves"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7. Personal para Destrucción de Información

Política: La destrucción de información sensible debe ser llevada a cabo por personal de la Empresa X o por una empresa garantizada de servicios de destrucción.

Comentario: Esta política garantiza que un individuo u organización confiables estarán encargados de la destrucción de la información confidencial. Se han visto casos en que las empresas encargadas de la destrucción de información no han triturado la información sensible y la han depositado en vertederos de basura, para ser luego descubierta por terceros. Para evitar este tipo de problemas, esta política garantiza que se han verificado los antecedentes del empleado o empresa encargada de la destrucción de la información y que están asegurados. Esta política debe utilizarse conjuntamente con otras políticas que establezcan los métodos de destrucción.

Políticas Relacionadas: "Disposición de Información en Papel"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Cajas para la Destrucción de Información Sensible

Política: Toda la información secreta, confidencial y privada que ya no se utilice o necesite, debe colocarse en cajas metálicas bajo llave hasta que la recoja el personal autorizado de la Empresa X o el servicio de destrucción contratado.

Comentario: Esta política garantiza que la información confidencial no caerá en manos no autorizadas cuando vaya a ser destruida. Cantidad de información que esperan ser eliminadas representan un objetivo atractivo

para los espías industriales, empleados curiosos y otros. Las cajas mencionadas en la política lucen como un buzón de correos público y tienen el tamaño y el peso adecuado como para no ser robadas fácilmente. Para evitar el robo de la caja, en algunos casos las cajas son encadenadas, cerradas o atornilladas al piso u otro mueble. Esta política supone que las personas responsables de la eliminación clasificarán el material con base en consideraciones de reciclaje. En algunos casos se aconseja tener recipientes separados para los distintos materiales sensibles a ser reciclados. Esta política debería utilizarse junto con otras políticas que especifiquen cómo debe ser destruida la información.

Políticas Relacionadas: "Disposición de Información en Papel"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9. Materiales Usados con Información Sensible

Política: Todos los materiales que se utilicen en el manejo de información sensible, incluyendo, sin limitantes, papel carbón, negativos fotográficos, rollos de fax de transferencia térmica, copias de impresiones interrumpidas y photocopies de mala calidad que pudieran contener información sensible, deben ser destruidos de la misma manera que la información sensible.

Comentario: Esta política impide que personas no autorizadas tengan acceso a información sensible al examinar los subproductos dejados por el manejo de la información confidencial. Si se vierten estos materiales sensibles en la basura, ésta puede ser revisada en busca de información. Mucha gente no está al tanto de que la información sensible puede ser divulgada de esta manera, así que se recomienda emitir una notificación en el sentido de tener cuidado con estos subproductos. La lista de subproductos incluida en la política puede ser ampliada para incluir los materiales relacionados con las tecnologías en uso en la Empresa X. Esta política asume que la palabra "sensible" está definida en otra política.

Políticas Relacionadas: "Destrucción de Materiales para Generación de Claves," "Disposición de Información en Papel," y "Clasificación de Datos en Cuatro Categorías"

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

8.06.03 Procedimientos para el Manejo de la Información

1. Acceso a Formularios

Política: El acceso a los artículos de papelería, los cheques en blanco y otros formularios de la Empresa X, debe estar disponible sólo a las personas que demuestren necesidad de acceso a tales formularios.

Comentario: La política notifica al personal que los formularios de la Empresa X se pueden utilizar para cometer delitos u otros actos no autorizados. Por ejemplo, se han producido muchos casos de cartas de crédito fraudulentas mediante el uso de los artículos de papelería. Pueden incorporarse a la política las distinciones en cuanto a los tipos de formularios que se han de restringir. Además de esta política, algunos formularios como los cheques impresos, deben ser guardados bajo llave cuando no estén en uso.

Políticas Relacionadas: “Formularios para Identificadores de Usuario”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Distribución de Materiales de Mercadeo

Política: Los trabajadores no deben utilizar las máquinas de fax, los correos electrónicos, los sistemas de voz de robot con marcador automático o cualquier otro sistema comunicacional electrónico para la distribución de material publicitario no solicitado.

Comentario: Esta política impide que el personal interno utilice las tecnologías de distribución de información con propósitos comerciales si el receptor no ha mostrado interés por los productos o los servicios de la Empresa X. Tales ofrecimientos son rechazados cada vez con más fuerza y molestia. En algunas jurisdicciones, estos ofrecimientos no solicitados pueden hasta ser ilegales. Esta política conserva la privacidad del público y es un potencial elevador de imagen siempre y cuando la política o la información sobre su existencia llegue a los oídos del público. La política podría ser ampliada al uso del teléfono, en cuyo caso las llamadas no solicitadas estarían en contra de la política interna. El sistema de correos no se consideró en la política para permitir correo masivo, ya que ésta es una práctica aceptada.

Políticas Relacionadas: “Bloqueo del Uso de Datos Privados”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

3. Divulgación de los Controles del Sistema Informático

Política: Los trabajadores no deben revelar a ninguna persona ajena a la Empresa X, ni los controles de los sistemas informáticos en uso ni la forma en que son implantados, sin la autorización del departamento de Seguridad Informática.

Comentario: Si se divulga la información relacionada con los controles, los terceros podrían utilizarla para reducir su tarea de intentar comprometer la seguridad de los sistemas informáticos. Se requieren esfuerzos de ingeniería social para obtener dicha información. En estos casos, los atacantes de los sistemas asumen postura de funcionarios gubernamentales, de empleados de la misma organización u otras personas autorizadas. Sin una política como ésta, los usuarios pueden tratar de ser útiles y de esta manera comprometer de manera no intencionada la seguridad. Esta política puede ser ampliada con ejemplos de los tipos de información que no deben ser revelados. Algunas organizaciones pueden ampliar esta política para que incluya aspectos de seguridad física. La política se podría mejorar si se añade una excepción con respecto a los auditores externos autorizados para recibir dicha información por un vicepresidente u otro gerente de alto rango. Esta política es pertinente para las discusiones técnicas en los salones de chateo de Internet, en las discusiones de grupo de Internet, en los foros electrónicos y en otros foros públicos. Estos foros pueden, por ejemplo, tratar los detalles de cómo instalar un cortafuego en la red. Es posible, y a menudo recomendable, que los empleados se involucren en tales discusiones técnicas sin suministrar información detallada en cuanto a los sistemas de su empresa. Los gerentes departamentales pueden verse en la necesidad de alertar a los usuarios que se involucran en estas discusiones de no revelar información detallada de manera no deliberada.

Políticas Relacionadas: “Comunicaciones Públicas,” “Divulgación de las Vulnerabilidades del Sistema Informático,” y “Números de Acceso a Computadores”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Remoción de Información Sensible

Política: La Información sensible de la Empresa X no debe ser removida de los límites de la Empresa X, a menos que exista una autorización previa del Propietario de la información.

Comentario: La política impide que la información sensible sea removida de las sedes de la Empresa X, lo que aumentaría el riesgo de divulgación de manera no autorizada. Mientras mayor tiempo permanece la información en un sitio, más fácil resultará rastrearla y controlarla. Esta política puede restringir las actividades de los teletrabajadores y de los empleados que deseen llevar trabajo a sus casas. Si tal información sensible viaja a través de redes de computación geográficamente dispersas, se puede dificultar la identificación de su ubicación en un momento determinado. Si participan teletrabajadores, o si la información de hecho está siendo intercambiada por redes dispersas geográficamente, será un tanto difícil y hasta poco apropiado poner en práctica esta política. Esta política asume que ya se ha adoptado un sistema de clasificación de datos. La palabra "sensible" podría ser reemplazada por uno o varios términos en uso en la organización.

Políticas Relacionadas: “Propiedad de la Información”, “Clasificación de Datos en Cuatro Categorías”, “Registro de Remoción de Información Sensible”, “Gabinetes Metálicos con Cerradura,” y “Recuperación de la Propiedad de la Organización”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

5. Información Secreta Fuera de Oficinas

Política: La información secreta de la Empresa X, sin importar su forma, no debe salir de las oficinas de la Empresa X sin la autorización de la gerencia de Seguridad Informática.

Comentario: Esta política garantiza que los trabajadores no se llevarán información secreta a sus casas para trabajar en ella, no la llevarán consigo en sus viajes de negocio, y bajo ningún concepto la expondrán de manera no autorizada fuera de los límites de la Empresa X. La presente es una política estricta que requiere la intervención de la gerencia de Seguridad Informática antes del traslado de la información. De conformidad con esta política, el gerente podría otorgar algunas excepciones a la política si el individuo en cuestión utiliza las medidas de seguridad adecuadas. Dichas medidas, de manera intencional, no se especifican en la política, de tal manera que si éstas cambian en el

tiempo, no existirá la necesidad de modificar la política. Esta política también brinda la oportunidad de enfrentar los riesgos de cada tipo de información secreta con un diferente conjunto de controles. Si la organización participa en extranets u otras redes multiorganizacionales similares, entonces esta política resulta poco práctica y podría ser reemplazada por una política que especifique las maneras de proteger la información secreta cuando se encuentre fuera de los límites de la Empresa X.

Políticas Relacionadas: “Remoción de Información Sensible en Papel,” “Áreas Desatendidas,” e “Inspección de Bolsos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

6. Registro de Remoción de Información Sensible

Política: Toda remoción de información sensible de las instalaciones de la Empresa X debe quedar plasmada en un registro con la fecha, la información propiamente dicha y las personas que poseen la información.

Comentario: Esta política mantiene un registro de toda la información sensible extraída de las instalaciones de la Empresa X. Tales registros servirán de apoyo en las investigaciones que sigan a la divulgación no autorizada de la información. El mantener un registro puede disuadir a los ladrones o a los empleados de extraer dicha información sensible. Esta política pudiera ser modificada con el fin de especificar quién debe mantener estos registros y si los Propietarios de la información deben ser notificados cuando la información sensible sale de las instalaciones de la Empresa X. La política, de manera intencional, no establece distinciones entre copias impresas y las otras maneras de representar la información. Para permitir que la política se aplique a una pequeña parte de la información dentro de una organización, la palabra "sensible" podría ser reemplazada por la palabra "secreta." Esta política asume que la información ha sido etiquetada apropiadamente con una designación de sensibilidad, así como supone la existencia de otra política con la definición de la palabra "sensible".

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Información Secreta en Computadores Portátiles,” y “Remoción de Información Sensible”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad:Todos

7. Liberación de Medios de Almacenamiento de Computación

Política: Los medios de almacenamiento de computación utilizados para grabar la información secreta no deben abandonar los canales controlados hasta haber sido desmagnetizados o sobrescritos, de conformidad con las normas publicadas por el departamento de Seguridad Informática.

Comentario: La política establece el concepto de un canal controlado para la custodia de la información secreta. La palabra "secreta" puede ser reemplazada con el término que defina el tipo de información. Un canal controlado en este contexto, es una forma de canalizar el manejo de la información con el fin de preservar su seguridad, lo cual puede involucrar a una o a muchas personas. La desmagnetización implica someter a los medios de almacenamiento magnéticos, tales como los discos flexibles, a fuertes campos magnéticos que borrarán la información allí almacenada. Sobrescribir los medios de almacenamiento con secuencias repetidas de ceros y unos hará que los datos desaparezcan de dichos medios. La política fomenta la idea de acuerdos de confidencialidad y del cifrado.

Políticas Relacionadas:“[Transferencia de Información Sensible](#)” y “[Destrucción de Información Sensible](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Medianos y altos

8. Areas Con Información Sensible

Política: Todas las oficinas de la Empresa X y las áreas donde se maneje información sensible deben contar con trituradores operativos.

Comentario: Esta política garantiza que las herramientas adecuadas para la destrucción de la información serán suministradas a quienes las necesiten. Los trabajadores a menudo reciben instrucciones sobre cómo destruir los datos sensibles con procedimientos especiales, pero no reciben las herramientas correspondientes. La política no sólo establece la presencia física de las máquinas trituradoras de papel, sino que además deben estar en buenas condiciones. La política previene las revelaciones masivas de información que ocurren cuando alguien revisa los receptores de basura de la organización. La intención de esta política es prevenir el espionaje industrial y los esfuerzos de otros terceros no autorizados.

Políticas Relacionadas: “Copias Sobrantes de Información Sensible,” “Requisitos de Seguridad para Teletrabajo,” y “Eliminación de la Información de Pago”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

9. Copia Maestra de Datos Críticos de Producción

Política: La copia maestra de los datos críticos de producción debe ser almacenada en uno o más servidores de producción y no en máquinas de escritorio.

Comentario: La política garantiza que la copia maestra no será almacenada en máquinas de escritorio donde existe la posibilidad de no tener un respaldo adecuado, no estar protegida contra cambios no autorizados, o ser divulgada de manera no autorizada. Dado que la mayor parte de la actividad empresarial se maneja en máquinas de escritorio o computadores personales, estas pequeñas máquinas también conservan la copia maestra de la información crítica. Los servidores de producción generalmente tienen mayor seguridad física, una administración de sistemas más profesional, mejores sistemas de detección de intrusiones y otras instancias de sistemas de seguridad más estrictos. La política supone que la organización se ha tomado el tiempo para establecer la distinción entre la información crítica y la no crítica, lo cual es una actividad muy importante que debe preceder cualquier esfuerzo relativo a planes de contingencia.

Políticas Relacionadas: “Servidores para Aplicaciones Críticas” y “Ubicación de Sistemas de Computación de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Divulgación de las Modificaciones a la Información

Política: Si la información emitida por la Empresa X se ha modificado de alguna manera, se deben notificar tales cambios a los receptores, antes de que éstos tomen decisiones basadas en dicha información.

Comentario: Esta política garantiza que los receptores de la información no tomarán decisiones equivocadas con base en la información modificada porque no entendieron o no estaban al tanto de los cambios. La

política exige que el departamento de Seguridad Informática notifique a los usuarios sobre los cambios en la información que aparece en sus reportes. La política se puede interpretar para que se aplique tanto a los consumidores internos de información como a los externos. El consumidor de la información es el que debe determinar si ciertos cambios son sustanciales y si alterarían o no sus decisiones.

Políticas Relacionadas: “Etiquetado de Datos Usados Como Base de Decisión Gerencial” y “Fotografías Alteradas”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Información de Contacto del Empleado

Política: Todos los trabajadores deben escoger una sola manera de mostrar su nombre, dirección y cualquier otra información personal y utilizarla de manera constante en todos los asuntos relacionados con la Empresa X.

Comentario: Esta política impide que se comparan en forma errónea los archivos pertenecientes a un mismo empleado. Por ejemplo, una base de datos puede tener un "S. M. Smith" mientras que otra puede tener un "Samuel M. Smith", pero quizás el software no puede detectar el hecho de que ambos nombres pertenecen a la misma persona. Una comparación errónea pudiera llevar a reportes imprecisos. Desde cierto punto de vista eliminando la necesidad de tener una política como ésta, algunos recientes paquetes de software tienen la capacidad de detectar posibles duplicados en las listas de correo y archivos similares. La explicación que debe acompañar a esta política debería establecer que los trabajadores tienen el derecho de hacer los cambios de información de índole personal que consideren pertinentes, sólo que deben hacerlo de manera consistente cada vez que ocurra un cambio.

Políticas Relacionadas: “Convenciones en Nombres,” “Integridad del Registro Personal,” y “Atributos de la Integridad de la Información”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

12. Transmisión de Datos Secretos

Política: Toda información secreta de la Empresa X transmitida a través de cualquier red de comunicación debe estar cifrada.

Comentario: Esta política prohíbe la transmisión de datos secretos no cifrados a través de una red que pudiera estar intervenida. El cifrado, también denominado codificación o aleatorización, oculta los datos de tal manera que terceros no autorizados no puedan leerlos. El cifrado también puede ser utilizado para indicar que un tercero envió un mensaje y que el mismo no fue modificado en tránsito, a menudo a través de firmas digitales, que son posibles gracias al cifrado. Esta política puede ser respaldada con un programa de cifrado a nivel de aplicación o a nivel de red. La política no especifica un algoritmo de cifrado, aunque algunas organizaciones optan por mencionar un algoritmo en la política. Esta política es importante para sistemas menores tales como los computadores personales, las redes de área local, los sistemas cliente-servidor e intranets, debido que a menudo los usuarios no están conscientes de la protección que requieren los datos secretos. Sin una política como ésta, existe la posibilidad de que los usuarios expongan datos secretos sin necesidad. Esta política supone que ya se ha implantado un sistema de clasificación de datos.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Algoritmo de Cifrado Normal e Implementación,” y “Envío de Información Sensible Vía Fax — No Cifrada”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

13. Transporte de Datos Secretos

Política: Toda información secreta transportada en medios de almacenamiento legibles por computador debe estar cifrada.

Comentario: Esta política prohíbe a los trabajadores transportar los datos secretos en medios de almacenamiento legibles por computador sin estar cifrados. El cifrado de estos medios no sólo oculta y encubre los datos, también se puede utilizar para detectar fallas en el sistema y manipulaciones. Cuando los medios de almacenamiento informáticos pasan a través de las máquinas de rayos X de los aeropuertos y se someten a otros campos magnéticos en la vía, existe la posibilidad de que se modifique o se borre parte de la información. Si los datos están cifrados, se va a hacer evidente de inmediato si estos están borrados o modificados, dependiendo del algoritmo de cifrado utilizado. Esta política asume que un sistema de clasificación de datos está activo.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Viajes con Información Secreta”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

14. Cifrado de la Información Secreta

Política: Toda la información secreta computarizada debe estar cifrada cuando no esté en uso.

Comentario: Esta política impide que la información secreta sea expuesta accidentalmente a personas no autorizadas. Si los datos cifrados fueron almacenados en forma no cifrada, pueden terminar en cintas de respaldo y ser visualizadas por personas no autorizadas. De esta manera pueden evitarse los controles normales de acceso. Por ejemplo, los computadores personales y las estaciones de trabajo pueden utilizar paquetes de software disponibles a nivel comercial para cifrado de antecedentes y cuyo uso es transparente para el usuario. Con estos paquetes, los datos del disco duro están cifrados, pero quedarán descifrados automáticamente al ser solicitados por una aplicación. Después de que un programa autorizado de aplicaciones cambie o utilice los datos, éstos son nuevamente escritos en el disco duro en forma cifrada. La única actividad del usuario es suministrar la clave de cifrado en el momento en que se inicia el sistema. Esta política asume que ya está activo un sistema de clasificación de datos.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Cifrado en Medios de Respaldo”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

15. Cifrado de Almacenamiento en Disco

Política: Todos los datos almacenados en discos duros deben estar cifrados a través de procesos transparentes para el usuario.

Comentario: Esta política impide que personas no autorizadas puedan acceder a los datos confidenciales propiedad de la Empresa X. Esta política no exige a los usuarios distinguir entre datos secretos y no secretos. Eliminar a los usuarios del proceso de toma de decisiones puede incrementar la seguridad, debido a que disminuyen las probabilidades de que tomen una decisión incorrecta. Al mismo tiempo, cifrar todos los datos va a implicar una mayor carga para los sistemas informáticos que el cifrado selectivo de datos y de esta manera se reduce el tiempo de respuesta del sistema.

Debido a que esta política define la vía más efectiva para la protección de los datos en un ambiente de computación distribuido, dicha política es particularmente importante para los computadores personales, las estaciones de trabajo, las redes de área local, las intranets y los sistemas cliente-servidor. Una alternativa a esta política es el uso de un desmagnetizador para borrar la información sensible almacenada en un disco duro antes de que el computador salga de la organización para reparación.

Políticas Relacionadas: “Cifrado de la Información Secreta,” “Almacenamiento de Información Sensible,” “Transferencia de Información Sensible,” y “Destrucción de Información Sensible”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

16. Descarga de Información Sensible

Política: Antes de transferir alguna información secreta, confidencial o privada de la Empresa X de un computador a otro, el trabajador que realiza la transferencia debe asegurarse de que los controles de acceso del computador receptor son proporcionales a los del computador remitente.

Comentario: Esta política exige que los usuarios consideren las consecuencias de descargar información sensible. La descarga de información se ha considerado un problema de seguridad debido a que los controles en los sistemas receptores pueden ser menos estrictos que los del sistema remitente. La descarga también puede ser un problema porque en muchas instancias, las etiquetas de sensibilidad de datos no se extienden de un sistema operativo a otro. Otra de las intenciones de la política es prohibir la descarga de información sensible que no esté protegida adecuadamente. En este sentido, la política es una manifestación del concepto de que la información debe ser protegida conforme a su sensibilidad, criticidad y valor, sin importar donde resida la información, quién la maneje y la forma que adquiera. La descarga puede realizarse en Internet, a través de una línea discada, a través de una oficina de servicio en línea y a través de otros métodos. Aunque implique cambios significativos en su redacción, esta política podría ser ampliada con el fin de incluir controles sobre buscapersonas alfanuméricos y otras formas que pueda adquirir la información una vez fuera de un sistema informático con controles de acceso. Esta política puede generar llamadas al departamento de Seguridad Informática debido a que los usuarios van a hacer preguntas acerca

de lo que significa "proporcional a" en la Empresa X. Una manera de reducir estos cuestionamientos es emplear categorías de control para los sistemas de seguridad tales como bajo, medio y alto, con una definición de los controles que acompañan a cada categoría. Esta política asume que las palabras "secreta, confidencial o privada" están definidas en otro sitio.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Protección de la Información”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

17. Autorización para Descargar Información Sensible

Política: La información sensible de la Empresa X no se debe descargar a un computador personal o a una estación de trabajo, a menos que exista una clara necesidad de negocio, así como una autorización previa del Propietario de la información.

Comentario: Cualquier información que un usuario de un sistema central, un minicomputador o de un servidor departamental pueda visualizar, al mismo tiempo puede ser capturada en un disco duro o un disco flexible o en un computador personal o en una estación de trabajo. Si no se cuenta con controles técnicos generalmente disponibles, esta política se puede aceptar para solventar este problema. La intención de la política es especificar las circunstancias bajo las cuales los trabajadores no deben descargar los datos. Por ende, las demás operaciones de descarga están permitidas. Esta política asume que la palabra "sensible" está definida.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Propiedad de la Información,” “Descarga de Información Sensible,” y “Descarga de Software”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

18. Devolución de Llamadas de Larga Distancia

Política: Los trabajadores de la Empresa X no deben devolver llamadas normales o responder llamadas de buscapersonas cuyos cargos puedan resultar mayores a los de una llamada telefónica normal o aquéllas de cargos revertidos.

Comentario: Los trabajadores deberían ser cautelosos en cuanto a posibles ardides que seducen al receptor con una llamada normal o de buscapersonas y que al ser devuelta resulte en cargos mayores por minuto de llamada. Esta política instruye a los trabajadores en el sentido de no devolver estas llamadas. La política podría ser ampliada para mencionar el colgar apenas oigan que serán cargados montos adicionales.

Políticas Relacionadas: “[Llamadas Cobro a Destino y a Terceros](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

19. Solicitudes Inusuales de Operación Telefónica

Política: Se deben denegar de manera consistente y diplomática las solicitudes poco usuales de operaciones telefónicas, tales como la llamada de una persona solicitando una línea externa, y los detalles de la llamada deben ser reportados inmediatamente al gerente del departamento de Telecomunicaciones.

Comentario: Esta política impide que terceros tomen ventaja de las características sofisticadas de los sistemas telefónicos para obtener una línea externa gratuita. Las solicitudes varían según la ubicación y el sistema telefónico utilizado. Estas conexiones son útiles para los hackers, los cuales querrán ocultar sus huellas y hacer que otros paguen por sus llamadas. Si el gerente de Telecomunicaciones recibe reportes sobre el número de llamadas con solicitudes poco usuales, puede emitir un memorando a todo el personal para recordarles la política al respecto. Esta política impide que los integrantes del personal sean víctima de estrategias de ingeniería social, donde quien realiza la llamada se hace pasar por alguien investido de autoridad.

Políticas Relacionadas: “[Informes de Actividad No Autorizada](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

20. Uso Personal del Teléfono

Política: Los teléfonos de la Empresa X no deben ser utilizados para fines personales, a menos que las llamadas no se puedan realizar fuera de horas laborables, en cuyo caso deben tener una duración razonable.

Comentario: Esta política clarifica lo que constituye un comportamiento aceptable en cuanto al uso del sistema telefónico para fines personales. Esta política representa una postura práctica que refleja una mezcla entre la postura estricta de que los teléfonos no deben ser utilizados para fines personales y la de reconocer que los trabajadores tendrán en algún momento la necesidad de realizar llamadas personales. Un enfoque más estricto implica la prohibición de todo uso personal del teléfono, a menos que se relacione con asuntos personales. La política más estricta hace énfasis en la reducción de los costos telefónicos, mientras que las dos versiones ayudan a incrementar la productividad de los trabajadores.

Políticas Relacionadas: “[Uso Personal de los Sistemas de Computación y de Comunicaciones](#),” “[Uso Personal de Internet](#),” y “[Usos del Sistema de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

21. Llamadas Telefónicas Personales de Larga Distancia

Política: Los teléfonos de la Empresa X no deben ser utilizados para realizar llamadas personales de larga distancia, a menos que las llamadas sean de una duración razonable, notificadas a la gerencia y compensadas a la empresa.

Comentario: Esta política clarifica el uso de los teléfonos de la Empresa X para fines personales, especialmente para llamadas de larga distancia. El énfasis en larga distancia es conveniente debido a que es allí donde se concentran los mayores gastos en llamadas personales. Esta política permite de manera implícita las llamadas personales sin necesidad de notificarlas ni reembolsarlas. Algunas organizaciones pueden añadir una condición adicional donde exigen a los empleados el uso de un código contable especial para indicar que las llamadas son personales. En este caso, se les puede presentar una lista de llamadas personales a ser canceladas o se les puede deducir directamente de su sobre de pago. Sin el código contable introducido en el momento de la llamada, será difícil en muchas ocasiones determinar cuáles llamadas fueron personales y cuáles relacionadas con el negocio. Las palabras “duración razonable” son utilizadas en esta política para mantener al mínimo el impacto sobre la productividad.

Políticas Relacionadas: “[Uso Personal del Teléfono](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

22. Intercambio de Información por Internet

Política: El software de la Empresa X, la documentación y demás tipos de información, no deben ser vendidos ni transferidos a ningún ente que no pertenezca a la Empresa X con otro propósito que no sea el comercial, autorizado expresamente por la gerencia.

Comentario: La intención de esta política es prohibir el intercambio no autorizado de información interna a través de Internet. Las organizaciones se sorprenden de que sus trabajadores han estado revelando información que la gerencia considera confidencial. La emisión de una política en cuanto a la divulgación de información de los clientes ayuda a los gerentes a descubrir que cierta información puede ser vendida por empleados a terceros.

Políticas Relacionadas: ‘Convenios de Intercambio de Software y Datos,’ ‘Publicación en Internet de Material,’ y ‘Responsabilidad en la Seguridad Informática’

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

23. Números de Cuenta Bancaria

Política: Los números de las cuentas bancarias de la Empresa X son confidenciales y no se deben revelar de ninguna manera a terceros.

Comentario: Individuos no autorizados pueden fácilmente cometer fraudes al introducir números de cuentas bancarias disponibles públicamente en formularios automáticos de solicitud de débitos. Esta política asume que la organización que adopta la política posee tanto cuentas de ahorro como cuentas de

crédito que pueden ser colocadas en formularios, así como instrucciones de transferencias bancarias a los clientes y cuentas de desembolso o de débito bancario. Cuando se adopta una política como ésta, las organizaciones deben hacer arreglos para rechazar los débitos a cuentas reservadas para fondos entrantes o cuentas de crédito.

Políticas Relacionadas: ‘Números de Acceso a Computadores’

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos

24. Seguridad de la Información Sensible

Política: Todos los medios de almacenamiento de información que contengan información sensible, deben estar físicamente seguros cuando no estén en uso.

Comentario: Esta política exige a todos los gerentes locales implantar medidas de seguridad física o de cifrado para la información sensible. Esta política es muy importante para los computadores portátiles, laptops, PC de bolsillo y otros computadores personales pequeños. El cifrado se exige porque no se puede garantizar la seguridad física al trasladar estos sistemas de un edificio a otro. Esta política evita los robos de los computadores personales contentivos de información sensible. Esta política puede ampliarse para incluir información valiosa o crítica

Políticas Relacionadas: ‘Acceso a Sistemas de Computación y Comunicación,’ ‘Cifrado de Almacenamiento en Disco,’ e ‘Información Secreta en Correo Electrónico’

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

8.06.04 Seguridad de la Documentación del Sistema

1. Entrega de Documentación de Sistemas

Política: Previo a ser expuesta a terceros, toda la documentación que describa los sistemas informáticos de la Empresa X o los procedimientos de los sistemas debe ser revisada por la gerencia de Seguridad Informática.

Comentario: Es importante transmitir a los trabajadores que la documentación, además de los registros comerciales, puede exigir procedimientos estrictos de difusión. Esta política informa a los integrantes del personal que no deben publicar la documentación interna de los sistemas sin autorización previa. Es también importante esta política debido a que varios hackers de sistemas utilizan la ingeniería social para obtener información en cuanto a sistemas internos, lo cual les permite entrar de manera forzada a estos

sistemas. Si se notifica a los empleados que tal información no se debe distribuir a terceros sin previa autorización, es menos probable que lo hagan. La existencia de sistemas de correo electrónico conectados a Internet también facilita la transmisión no autorizada de la documentación interna a terceros.

Políticas Relacionadas: “Liberación de Información de la Organización” y “Direcciones Internas de la Red”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

2. Confidencialidad de la Documentación

Política: Toda la documentación relacionada con los computadores de la Empresa X es confidencial y no debe ser trasladada a ningún otro sitio cuando el trabajador cesa su relación laboral con la Empresa X.

Comentario:Esta política impide que alguien que haya escrito algún tipo de material para la Empresa X se lleve la documentación consigo al momento de abandonar la

Empresa X. La política recuerda a los usuarios finales, al personal del departamento de Sistemas Informáticos y a otros, que la documentación relacionada con los computadores es confidencial y que no debe ser revelada a terceros sin el permiso de la gerencia. Debido a que ésta ha representado un área difícil, tanto en términos de comunicación entre la gente involucrada como en términos de leyes ambiguas, es importante especificar el arreglo en una política, en los contratos y en los otros documentos que correspondan. Si tal documentación llegara a las manos equivocadas, podría ser utilizada para violar los controles de los sistemas de la organización. El alcance de esta política podría ampliarse para incluir los sistemas de comunicación, tales como los operadores privados o las redes de área local.

Políticas Relacionadas:“Derechos de Propiedad”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

8.07 Intercambio de Información y Software

8.07.01 Convenios de Intercambio de Información y Software

1. Software Distribuido a Terceros

Política: Todo software desarrollado por la Empresa X para uso de posibles clientes, clientes, socios y otros, debe ser distribuido sólo en la forma de código objeto.

Comentario:La distribución en código fuente permitiría a los terceros utilizar inmediatamente el software con fines diferentes para los que fue originalmente concebido por la Empresa X. Por ejemplo, los compradores pueden terminar incorporando el código en un producto comercializado por ellos mismos. De la misma manera, dichos compradores pueden modificar el software sin autorización y de tal manera que funcione lenta e incorrectamente. Esta política no elimina la posibilidad de utilizar un compilador inverso para derivar un código fuente de un código objeto. Si bien no evita la ingeniería inversa, la distribución en forma de objeto dificulta mucho más este uso no autorizado. También se recomienda el uso de otras medidas de control para evitar las copias y la ingeniería inversa, tales como el cifrado y la dependencia en los parámetros legibles por software, tales como el número de serial del computador. Esta política respalda a la Empresa X en su

intento de probar en un tribunal el uso de los controles adecuados para mantener el software como secreto industrial.

Políticas Relacionadas:“Garantía Especial de Software” y “Convenios de Software con Terceros”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

2. Convenios de Software con Terceros

Política: Todo software desarrollado por la Empresa X para su uso por posibles clientes, clientes, socios y otros, sólo se puede distribuir una vez que los receptores hayan firmado un acuerdo estableciendo que no van a desarmar, a utilizar ingeniería inversa, a modificar o a utilizar el programa en contravención a lo acordado con la Empresa X.

Comentario:Esta política genera acuerdos por escrito en cuanto al uso autorizado del software desarrollado por la Empresa X previo a su distribución. Ello impedirá el robo de la propiedad intelectual de la Empresa X o un

uso para el que no fue diseñada. La política se aplica en organizaciones cuya actividad principal no es la venta o el desarrollo de software, mientras que en las organizaciones para las que estas actividades constituyen su negocio principal, tendrán que llegar a acuerdos de mayor formalidad y legalidad. Algunas organizaciones querrán añadir otra condición a esta política que trate sobre excepciones. Un ejemplo podría ser un programa sencillo para hacer llamadas, que permita a los clientes llamar a un computador de la Empresa X y verificar el estado de una orden. El desmontaje es más o menos lo mismo que una compilación inversa, porque la diferencia la establece el tipo de lenguaje de programación utilizado. Ingeniería inversa significa deducir el funcionamiento interno de un producto a partir de su funcionalidad aparente.

Políticas Relacionadas: “Software Distribuido a Terceros” y “Responsabilidades de Terceros en la Seguridad Informática”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Convenios de Intercambio de Software y Datos

Política: Los intercambios de software o información interna entre la Empresa X y los terceros deben estar acompañados por un acuerdo escrito que especifique los términos del intercambio y la manera en que el software o la información se manejará y protegerá.

Comentario: Esta política evita malos entendidos en cuanto al uso o la protección de la información sensible de la Empresa X. Por ejemplo, si dos empresas intercambian listas de correos internas, se podría especificar por escrito que las listas serán utilizadas una sola vez. Tener un contrato escrito también evita difundir la información a terceros no autorizados y ser utilizada para objetivos para los que no fue diseñada. Debido a que promueve cierto control sobre la difusión de la información, esta política resulta importante para los correos electrónicos, los foros electrónicos e Internet. Se puede conceder una excepción dentro de la política. Las solicitudes de datos del gobierno, tales como la emisión de un decreto, no necesitan acuerdos. Puede que algunas organizaciones quieran incorporar palabras específicas en cuanto a ciertos tópicos a los cuales hay que hacer referencia dentro de un acuerdo. Estos podrían incluir responsabilidades en cuanto a la seguridad de las partes en cuestión, a los procedimientos para proteger el software o la información y a la asignación de los derechos de autor y otros derechos de propiedad intelectual.

tual. Esta política podría ser restringida para que sólo haga referencia a la información confidencial y a la privada.

Políticas Relacionadas: “Contratos Obligatorios en Sistemas Electrónicos” e “Intercambio de Información por Internet”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

4. Certificado de Destrucción de Medios de Almacenamiento

Política: Cada vez que una entidad externa que suministre información a través de medios de computación solicite que estos medios sean reintegrados, el personal de la Empresa X debe proporcionar al ente externo una garantía escrita de que todas las copias de la información han sido destruidas.

Comentario: Esta política evita que la información de la Empresa X se difunda accidentalmente a organizaciones externas. La razón es que se pudieron haber utilizado los medios de computación externos para almacenar temporalmente información sensible de la Empresa X, la cual pudo no haber sido destruida antes de que los medios fuesen devueltos. De una manera transparente para el usuario, el sistema operativo pudo también haber utilizado los medios para almacenar archivos contenitivos de información sensible. También puede ser que los medios contengan un programa que recopile información acerca de la Empresa X, realizando en efecto espionaje industrial, posiblemente bajo el artificio de un disco de demostración. El único método confiable para impedir este tipo de divulgación de la información sensible de la Empresa X es conservando los medios. Los proveedores de software u otros proveedores de información son más proclives a aceptar una declaración escrita sobre la destrucción del material involucrado en lugar de aceptar la devolución del medio de computación. Se podría moderar la política al solicitar tal destrucción del material en vez de sólo aceptar su devolución, si los medios de almacenamiento de datos pudieran ser modificados. La política podría ser modificada de manera que exija al personal de la Empresa X publicar la política antes de recibir los medios de almacenamiento de las entidades externas. Dado que resulta normal en algunas industrias no aceptar devoluciones de las entregas, como en la industria de la publicidad, las notificaciones previas no son necesarias. La política es importante sólo para aquellas organizaciones con necesidades estrictas de seguridad.

Políticas Relacionadas:“Transferencia de Información Sensible”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Altos

5. Contratos en Línea con Intercambio de Papel y Firmas

Política: Cada vez que terceros acepten una oferta en línea de la Empresa X, estos terceros deben suministrar sus firmas autógrafas en papel vía correo normal o a través de un servicio de mensajería.

Comentario: Esta política garantiza que no se presentarán conflictos legales asociados con la constitución de un contrato a través de las redes informáticas. En algunas jurisdicciones, las firmas digitales o los registros que notifican que un cliente pulsó el botón "OK" no representan evidencia suficiente para demostrar que un cliente tiene la intención de constituir un contrato. Aun con la tecnología actual, la firma autógrafa se considera la vía más conservadora y segura de constituir contratos. Este enfoque no disminuye el impulso que le imparte la informática a los negocios y garantiza la actualización del papeleo legal. Esto tendrá importancia en caso de un litigio. A ese nivel, la Empresa X puede apuntar tanto hacia el equivalente electrónico de una firma como a una firma autógrafa como evidencia de la intención del cliente de constituir un contrato. La política es intencionalmente vaga en cuanto a terceros, debido a que éstos pudieran ser otros terceros diferentes de los clientes. La política se podría generalizar al cambiar las palabras sobre las aceptaciones de los terceros para incluir tanto las ofertas como las aceptaciones.

Políticas Relacionadas:“Almacenamiento de Registros Vitales” y “Firmas en Correo Electrónico”

Política Dirigida a: Gerencia y personal técnico

8.07.02 Seguridad de Medios en Tránsito

1. Entrega por Terceros de Información Secreta

Política: No se debe enviar información secreta no cifrada a través de terceros, incluyendo, sin limitantes, servicios de mensajería, servicios de correo, compañías de teléfono y proveedores de servicios Internet.

Ambientes de Seguridad: Todos

6. Validación de la Identidad de Terceros

Política: Antes de que los trabajadores publiquen la información interna de la Empresa X, constituyan algún contrato o soliciten algún producto a través de las redes públicas, la identidad de los individuos y de las organizaciones contactadas debe ser verificada a través de certificados digitales, cartas de crédito, referencias de terceros o conversaciones telefónicas.

Comentario: La política notifica a los trabajadores que deben realizar una verificación completa antes de confiar en la identidad supuesta de aquellos con quienes intercambian información a través de las redes públicas. La confirmación de la identidad no se encuentra en Internet y se debe obtener a través de los controles agregados por las organizaciones usuarias. Una vía para obtener la confirmación de la identidad de otros usuarios es a través de los certificados digitales, ya que constituyen el equivalente de un pasaporte de Internet, siempre que un tercero haya dado fe de la identidad de un individuo o de una organización. Los certificados digitales permiten la elaboración de firmas digitales, las cuales evidencian que un mensaje no fue modificado en el camino y que definitivamente provino del individuo y la organización originarias. El uso de sistemas de cifrado que incorporan rasgos de autenticación proporcionan vías alternas para confirmar la identidad de los que intercambian correspondencia en Internet.

Políticas Relacionadas:“Autentificación de Contraseña en Persona,” “Divulgación en Internet de Información de Contacto,” y “Autentificación de Usuario Que Accede Vía Telefónica”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

Comentario: Esta política garantiza que la información secreta no llegará a manos de terceros no autorizados. La política obliga a los internos de confianza a llevar la información consigo o hacerla ilegible a través del cifrado. La política se restringe a la información secreta. La información menos sensible puede ser transmitida a través de terceros cuando se encuentre en formato legible.

Políticas Relacionadas:“Transmisión de Información Secreta en Papel” y “Uso de Mensajeros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

2. Viajes con Información Secreta

Política: Los trabajadores no deben viajar en transporte público cuando lleven consigo información secreta de la Empresa X, a menos que hayan sido autorizados por la gerencia.

Comentario: Esta política evita que la información secreta caiga en las manos equivocadas al viajar en transporte público, lo cual incluye aviones, trenes, tranvías, autobuses y sistemas subterráneos. Al disminuir la circulación de la información secreta, se reduce la probabilidad de que ésta sea ubicada por un tercero no autorizado. La flexibilidad de los horarios de trabajo y de las ubicaciones se puede ver restringida indirectamente como resultado de esta política. Los teletrabajadores y los empleados que deseen trabajar en sus hogares pueden considerar problemática esta política, lo que no significa que se deban paralizar los trabajos fuera del área de oficina. La solución puede ser extraer sólo la información que no sea secreta. Otra opción podría ser cifrar toda la información secreta que se encuentre fuera de la oficina o de otras áreas físicamente protegidas. La palabra "secreta" podría ser reemplazada por "sensible" o por un conjunto de términos determinados por la clasificación de datos utilizada en la organización. La política asume que el término "secreta" ya ha sido definido.

Políticas Relacionadas:“Clasificación de Datos en Cuatro Categorías,” “Computadores Portátiles en Aviones,” “Transporte de Datos Secretos,” y “Remoción de Información Sensible”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

3. Transporte Internacional de Información Secreta — Seguridad

Política: Cada vez que la información secreta sea trasladada por un trabajador de la Empresa X a un país extranjero, la información se debe almacenar en una forma no accesible o debe permanecer en manos del trabajador en todo momento.

Comentario: Esta política impide que los agentes de inteligencia obtengan información secreta. No se aconseja que tal información se deje en las habitaciones de los hoteles, a menos que esté cifrada. Toda información secreta almacenada en un computador debe estar cifrada. No se recomienda almacenar la información secreta en papel, porque puede ser fácilmente fotocopiada, fotografiada o digitalizada con un sistema de reconocimiento óptico de caracteres. La palabra "secreta" podría ser reemplazada por "sensible" o por un conjunto de clasificación de datos utilizado por la organización. En la política se asume que el término "secreta" ha sido ya definido.

Políticas Relacionadas:“Clasificación de Datos en Cuatro Categorías” y “Remoción de Información Sensible en Papel”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

4. Transporte Internacional de Información Secreta — Autorización

Política: Los trabajadores de la Empresa X no deben trasladar información secreta de la empresa a otro país, a menos que hayan sido autorizados por el gerente de Seguridad Industrial.

Comentario: El objetivo de esta política es prohibir el transporte no autorizado de información secreta a otro país. Un cambio de país trae consigo distintas leyes, por efecto de las cuales el espionaje industrial se puede considerar legal o por lo menos tolerable. Las organizaciones pueden afrontar problemas en sus intentos de alegar derechos legales en otro país. Esta política trata de evitar este tipo de problemas. La palabra "secreta" puede ser reemplazada por palabras parecidas en uso por la organización. La referencia a "gerencia de Seguridad Industrial" podría ser cambiada por gerencia de Seguridad Informática o por otro gerente que conozca sobre las leyes y los riesgos pertinentes. La política es definitiva en cuanto a que no menciona la forma que adquiere la información. Un problema de importancia para varias empresas, especialmente las de alta tecnología, ha sido emplear trabajadores de países extranjeros, que luego retornan a sus países con información secreta propiedad de la empresa. Aunque esta política no puede impedir esta actividad, puede aclarar que tal información no debe ser extraída del país sin un permiso especial. Esta política puede ser difícil de poner en práctica en empresas transnacionales que transportan información secreta alrededor del mundo durante su actividad comercial normal.

Políticas Relacionadas: “Transporte Internacional de Información Secreta — Seguridad,” “Remoción de Información Sensible en Papel,” y “Extranjeros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

5. Remoción de Información Sensible en Papel

Política: Cada vez que una versión en papel de la información sensible sea extraída de los alrededores de la Empresa X, ésta debe ser transportada en un maletín de mano o en un contenedor cuando no esté en uso y no debe dejarse desatendida en vehículos, en cuartos de hotel, en oficinas ni en ninguna otra localidad, aun cuando el vehículo o el cuarto estén bajo llave.

Comentario: Esta política notifica a los Custodios sobre la forma segura de manejar la información sensible en copia impresa en papel. Los pasos definidos en esta política evitan que la información sensible caiga en manos de hackers, de espías industriales, de la competencia y de otros que puedan tener intereses opuestos a los de la Empresa X. Esta política puede ampliarse para incluir discos flexibles y otros medios de almacenamiento no cifrados.

Políticas Relacionadas: “Información Secreta en Computadores Portátiles,” “Registro de Remoción de Información Sensible,” y “Transporte Internacional de Información Secreta — Seguridad”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

6. Transferencia de Información Sensible

Política: Todos los medios de almacenamiento de computación enviados desde la Empresa X hasta un tercero, no deben haber sido previamente utilizados y de haberlo sido, deben haber sido desmagnetizados o sobrescritos repetidamente antes de grabar en ellos la información a ser transferida.

Comentario: Esta política garantiza que la información residual, que pudo haber sido borrada, no permanecerá en el medio de almacenamiento y por lo tanto evita ser recuperada por un tercero. Esta política se aplicaría, por ejemplo, no sólo a los discos de demostración que se envían a los clientes potenciales, sino también a aquellos casos en los que los discos duros de los computadores viejos son enviados a entes de caridad. La información eliminada de un disco flexible se puede recuperar fácilmente a través de paquetes de utilidades disponibles comercialmente. Del mismo modo, aun cuando haya sido sobreescrita, la información almacenada en cintas magnéticas se puede recuperar con el uso de un equipo especial. La desmagnetización es uno de los mecanismos más seguros, porque somete los medios a campos electromagnéticos muy fuertes que definitivamente borran la información previamente almacenada. La repetición de ceros y unos borra la información previamente almacenada en los medios. En ambientes de muy alta seguridad, la sobreescritura repetida de los medios puede no brindar la protección adecuada. Esta política puede limitarse a aquellas circunstancias en las cuales se ha grabado información confidencial con anterioridad en los medios.

Políticas Relacionadas: “Certificado de Destrucción de Medios de Almacenamiento,” “Medios de Almacenamiento de Información Sensible,” y “Liberación de Componentes Usados”

Política Dirigida a: Todos

Ambientes de Seguridad: Altos

8.07.03 Seguridad del Comercio Electrónico

1. Obtención de Información desde Archivos Cookie

Política: La Empresa X no debe obtener información desde los archivos cookie colocados por otras organizaciones en cualquier disco duro, en su intento por conocer los sitios visitados por los usuarios de Internet.

Comentario: Esta política garantiza a los usuarios que los sistemas ubicados por la Empresa X en Internet, no examinarán clandestinamente los contenidos de los computadores de los clientes para luego revelar sus hábitos de navegación en la web. Es factible examinar los cookies colocados por otros proveedores o simplemente determinar qué tipos existen, con la intención de conseguir un perfil que revele los sitios visitados por un cliente. Recopilar esta información sin obtener previa-

mente el permiso por parte del cliente, puede constituir una violación de la privacidad. La política garantiza a los clientes que la Empresa X no se dedica a este tipo de prácticas. Publicar una política como ésta en Internet no compromete a la Empresa X ya que en el futuro, si se desea recolectar esta información, se debería por lo menos informar a los usuarios.

Políticas Relacionadas: “Cookies en Internet” y “Cookies para Inicios Automáticos de Sesión”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Clasificación de Contenido y Protección de la Privacidad

Política: La Empresa X debe adoptar y respaldar todas las normas de clasificación de contenidos, la protección de la privacidad de los sitios web y la seguridad del comercio en Internet.

Comentario: Esta política garantiza a los clientes que pueden colocar de manera segura las órdenes de compra de productos y servicios a través de Internet u otros sistemas en línea. La política está redactada de tal manera que puede ser publicada en un sitio web como parte de una declaración formal de privacidad. Se puede utilizar un cronograma de clasificación de contenido para definir la naturaleza de los contenidos en un sitio web, con etiquetas fácilmente legibles por el software de las organizaciones usuarias remotas, que filtran el material inaceptable de los sitios web.

Políticas Relacionadas: “Cookies”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Posibilidad de Rechazo de Comunicación de Mercadeo

Política: Toda publicidad escrita, dirigida a posibles clientes incluidos en la base de datos de contacto de la Empresa X, debe incluir palabras que indiquen claramente cómo el cliente puede evitar recibir más comunicaciones, correos o mensajes electrónicos no solicitados.

Comentario: Esta política garantiza que el correo normal, el correo electrónico basura y cualquier otro tipo de publicidad escrita no solicitada, incluirán un mecanismo que permita a los receptores evitar la

recepción de comunicaciones adicionales. En relación al correo electrónico, este mecanismo generalmente se encuentra al final del mensaje y los receptores pueden simplemente responder a la dirección del remitente. Esta política evita que la gente proteste por la cantidad de solicitudes que reciben y que prefieren no ser molestados, lo cual es un aspecto importante de la privacidad. Esta política no se aplica a listas de correos en alquiler y a otras bases de datos de terceros, debido a que la Empresa X generalmente tiene poco control sobre la actualización de dichas listas. La política se podría modificar para describir cuáles solicitudes se deben eliminar antes de ser retransmitidas a terceros.

Políticas Relacionadas: “Opción de Participación en Sistema de Datos Privados” y “Servicio Nuevo o Mejorado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Colocación de Clientes y Prospectos en Listas de Correos

Política: La Empresa X debe recibir una solicitud de un tercero interesado y reconfirmar dicho interés antes de colocar a este tercero en la lista de correos de cualquier empresa.

Comentario: En esta política se asume la postura de estar a favor del consumidor y de la privacidad, que en definitiva es beneficioso para el negocio, porque demuestra que la organización adoptante de la política siente verdadera preocupación por el respeto a los derechos de las personas. La política también demuestra que la organización adoptante de la política se preocupa por la integridad de los datos, específicamente se asegura de que sus registros internos estén correctos. La política sigue el ejemplo de varias organizaciones que han construido sus empresas sobre la elaboración de listas personales, en las cuales el receptor quiere recibir información sobre ciertos tópicos. La política se puede aplicar a una amplia variedad de organizaciones, no sólo aquellas que están elaborando sus listas de correo. Esta política también impide que una persona firme por otra, para que esta otra reciba comunicaciones no deseadas.

Políticas Relacionadas: “Autorización para Inclusión en Sistemas de Datos Privados” y “Distribuciones de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Almacenamiento en Servidores Web y Comerciales

Política: Los servidores web y los servidores comerciales no deben ser utilizados para almacenar información comercial crítica de la Empresa X.

Comentario: Esta política evita el deterioro de la información crítica. Las organizaciones no deben colocar su información crítica en las instalaciones de sus redes en las cuales se podrían deteriorar o ser modificadas por terceros no autorizados. La información crítica, como una base de datos de clientes, debería estar almacenada en máquinas internas ubicadas detrás de los cortafuegos adicionales u otras barreras de seguridad. Los servidores web y los comerciales pueden procesar la información crítica. Esta política asume que los servidores web y los servidores comerciales podrían ser dañados por un hacker sin impactos adversos a la organización. Se aconseja almacenar las cantidades grandes de información en máquinas seguras ubicadas detrás de varios niveles de control de acceso.

Políticas Relacionadas: “[Cortafuegos de Servidores Web](#)” y “[Cortafuegos de Servidores Comerciales de Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Verificación del Cálculo de la Cuenta

Política: Todos los clientes, los empleados y otros receptores de los cálculos realizados a su cuenta por la Empresa X, deben recibir información suficiente para verificar por su propia cuenta la exactitud de los cálculos.

Comentario: Esta política intenta brindar a los individuos información suficiente para que verifiquen si los cálculos fueron realizados correctamente. Esto se recomienda ya que se utiliza un tercero para ayudar a descubrir fraudes y fallas. Por ejemplo, un cliente bancario debería estar en capacidad de calcular los intereses que le cobran y de notificar a la gerencia al identificar un error. Esta política se recomienda además ya que disminuye la necesidad de personal de atención al cliente. Si los clientes tienen la información que necesitan para verificar sus cálculos, no necesitan contactar al departamento de atención al cliente. También se recomienda esta política ya que ayudará a fomentar buena voluntad y confianza en los clientes. Esta política no se aplica en organizaciones tales como las sociedades. Las normas contables definen la preparación de estados financieros y representan la

fuente de divulgación de los estados contables. De todos modos se recomienda aplicar este concepto a las organizaciones para evitar conflictos y habilitar mecanismos de verificación por parte de terceros, lo cual puede resultar muy útil en la identificación de fraudes, fallas, malos entendidos en las cláusulas de los contratos y otros problemas.

Políticas Relacionadas: “[Notificación de Falla en los Controles de la Integridad](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Confirmación de Cambio Solicitado por Cliente

Política: Todo cambio iniciado por un cliente en cuanto a su relación con la Empresa X, debe ser inmediatamente acusado como recibido a través de correo electrónico, carta u otro tipo de confirmación escrita.

Comentario: Esta política impide el fraude o por lo menos lo detecta rápidamente y por lo tanto minimiza las pérdidas. Si el cliente no autorizó dicho cambio después de recibir la notificación, se supone que contactará rápidamente a la Empresa X. El cambio en la relación a la que hace referencia la política, podría adquirir muchas formas, tales como la compra de productos, el cierre de una cuenta, la transferencia de dinero de una cuenta a otra o un cambio de dirección. Para evitar un incremento en los costos operacionales, la gerencia puede decidir que las notificaciones no son necesarias en algunos casos debido al bajo riesgo de fraude. Por ejemplo, si un cliente llama a la Empresa X y suministra un número para una tarjeta de crédito nueva, de tal manera que pueda seguir recibiendo el servicio, entonces la gerencia podría decidir que no existe necesidad de solicitar la confirmación del cliente. La dirección para el envío de la notificación de acuerdo a lo discutido en esta política no debe estar basada exclusivamente en la información nueva suministrada en el cambio. Por ejemplo, una nueva dirección de correo electrónico definida en un explorador de Internet no se debe tomar como la dirección definitiva, y la información debe ser enviada tanto a la dirección anterior como a la nueva.

Políticas Relacionadas: “[Cambios en la Sensibilidad, Criticidad y Valor de la Información](#)” y “[Confirmación de Cambio de Dirección](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Investigación de Errores

Política: Los errores detectados por los clientes en los registros de la Empresa X se deben investigar, corregir y resolver inmediatamente, dentro de un período de dos semanas, y acompañarse de una carta que especifique: que el cambio fue llevado a cabo de acuerdo a lo solicitado, que no se llevó a cabo la modificación y la razón correspondiente o la fecha de cuándo se llevará a cabo tal cambio.

Comentario: Esta política genera lealtad del cliente y mantiene vigentes los registros de la Empresa X. Dicha empresa establece un tiempo de respuesta para responder al cliente y comunicar a los trabajadores de la Empresa X que es importante que las respuestas sean dadas oportunamente. Aun cuando no se decida en forma definitiva acerca de un cambio, se debe informar al cliente de que la Empresa X está trabajando en el caso. Esta política podría ser ampliada para incluir los errores detectados por terceros. El énfasis en los clientes se justifica porque no sólo preocupa al público contar con unos registros de datos personales precisos, sino porque las relaciones con los clientes son un punto crítico para cualquier negocio.

Políticas Relacionadas: “Declaración Explicativa del Empleado,” “Errores y Manipulación de Registros,” “Entrada con Doble Tecla de Transacciones Mayores,” e “Integridad del Registro Personal”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9. Seguridad de los Servidores Comerciales en Internet

Política: Todos los servidores comerciales de Internet de la Empresa X, excepto los servidores que respaldan las comunicaciones con los clientes, los posibles clientes y otros integrantes del público, deben emplear certificados digitales individuales y deben utilizar el cifrado para transferir información entre los servidores.

Comentario: Esta política genera un alto nivel de seguridad en las comunicaciones entre los servidores comerciales de Internet y cualesquiera máquinas internas que permitan la comunicación entre estos servidores. Los certificados digitales se utilizan para identificar cada máquina de manera individual y las comunicaciones cifradas se utilizan para proteger la comunicación en tránsito. Las excepciones son necesarias debido a que las comunicaciones externas, tal

como la navegación normal en la web, no implican normalmente el uso de certificados digitales o el cifrado de la información.

Políticas Relacionadas: “Cortafuegos de Servidores Web” e “Instalación de Software Antivirus”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10. Servicio Nuevo o Mejorado

Política: Los clientes que reciban servicios de computación o de comunicaciones de la Empresa X, deben estar explícitamente de acuerdo en recibir servicios nuevos o mejorados antes de que éstos sean suministrados.

Comentario: Esta política conserva buenas relaciones con los clientes y garantiza que los sistemas de computación y de comunicaciones de dichos clientes continuarán siendo compatibles con los sistemas de la Empresa X. La política requiere el soporte de todos los servicios previamente disponibles. Esto no impide a la Empresa X prestar servicios nuevos o mejorados. La política es importante para la seguridad porque garantiza que los controles anteriormente eficaces continuarán siendo efectivos. Esta política no permite que los proveedores de servicios obliguen a los clientes a utilizar nuevos servicios, aunque dichos clientes no estén listos para recibirlas. Esto implica entender las consecuencias que genera la seguridad del nuevo servicio. La política respalda además los esfuerzos relativos a planes de contingencia, debido a la necesidad de continuar el soporte de los servicios anteriores. Si los servicios nuevos o mejorados implican problemas mayores, la Empresa X siempre puede volver a los servicios anteriores. Esta política puede ser percibida por los gerentes de Procesamiento de Datos como muy estricta y puede ser redactada con el fin de incluir a los clientes, los proveedores y otros terceros, pero no a los usuarios del sistema interno. La política podría ser ampliada para incluir una cláusula de excepción en la cual los servicios iniciales no necesiten ofrecerse si se llega a un acuerdo con la alta gerencia de la Empresa X. Esto evitará que la Empresa X se vea en la obligación de ofrecer servicios obsoletos y costosos. En algunos aspectos, esta política se parece al proceso de aceptación o rechazo que utilizan los sistemas que manejan datos privados.

Políticas Relacionadas: “Opción de Participación en Sistema de Datos Privados” y “Autorización para Cambiar Paquete de Software de Producción”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad:Todos**11. Contratos Obligatorios en Sistemas Electrónicos**

Política: Todos los contratos que impliquen el intercambio electrónico de datos y otros sistemas de negocios electrónicos con terceros, deben ser constituidos a través de documentos en papel antes de realizar las transacciones de intercambio, compra o venta.

Comentario: Los contratos constituidos a través de mensajes electrónicos pueden considerarse no válidos desde el punto de vista legal. Algunas leyes exigen un documento, un escrito o una firma para que un contrato pueda ser considerado válido. Esta política garantiza que todo intercambio de datos electrónicos o de correos electrónicos asociados a contratos, intercambiados entre organizaciones son vinculantes desde el punto de vista legal. El abogado de la organización debería revisar esta política antes de ponerla en práctica. La política podría ser ampliada para incluir palabras que impliquen que los convenios con terceros deben ser autorizados por el departamento Legal.

Políticas Relacionadas:“Convenio de Redes con Socios de Negocios,” “Convenios de Intercambio de Software y Datos,” y “Firmas Legales”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos**12. Transacciones Internacionales de Negocios por Internet**

Política: Los trabajadores de la Empresa X no deben adquirir bienes y servicios de una organización extranjera a través de Internet, a menos que cuenten con la autorización del departamento de Compras.

Comentario: Esta política evita los fraudes, especialmente aquéllos con poca probabilidad de restitución o litigio. No todos los fraudes en Internet son de carácter local y si el fraude es efectuado por una empresa extranjera, el caso puede resultar costoso y de larga duración. Si la organización está dentro del mismo país, las soluciones del conflicto será más factible y efectiva en términos de costos. Esta política no está diseñada para impedir intercambios comerciales con organizaciones extranjeras a través de Internet. Si alguno ha de proceder, el departamento de Compras pudiera llevar a cabo una evaluación de los antecedentes de dichas

empresas y se podría establecer una infraestructura legal especial. Las compras en el extranjero se deben realizar de manera cautelosa, ya que existen grandes diferencias entre los sistemas legales de diferentes países. Esta política podría ser modificada para que sólo se aplique a las transacciones que superen un monto específico.

Políticas Relacionadas:“Procura de Hardware y Software” y “Contratos por Correo Electrónico”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos**13. Convenio de Redes con Socios de Negocios**

Política: Un convenio de sociedad, que fije los términos y las condiciones de uso, se debe negociar y autorizar por medio del asesor legal de la Empresa X antes de que los sistemas de computación de la Empresa X se utilicen en cualquier red computarizada de negocios.

Comentario: Un convenio de sociedad determina sobre quién recae la responsabilidad si se pierde un mensaje, si se daña el sistema, si ocurre un fraude o si se presenta otro problema. Esta política impide que la gerencia del departamento usuario llegue a un acuerdo con una red de negocios electrónicos sin haber aclarado adecuadamente los términos y condiciones del mismo. Esta política garantiza la existencia de un control centralizado sobre los convenios de negocios en la red. Dicho control centralizado también brinda la oportunidad de revisar las medidas de control del sistema antes de su uso. Se debería consultar a los asesores legales sobre los detalles en cuanto a los convenios de sociedad. Una política de este tipo también resulta útil al momento de definir el significado de las firmas digitales y de los códigos de autentificación de los mensajes utilizados para los mensajes comerciales en red y otras transacciones que se manejan a través de sistemas multiorganizacionales. Esta política está redactada intencionalmente en sentido generalizado, para que se pueda aplicar en la constitución de contratos de manejo de negocios en Internet con un solo proveedor, un cliente o un socio.

Políticas Relacionadas:“Contratos Obligatorios en Sistemas Electrónicos”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

14. Contratos por Correo Electrónico

Política: Todos los trabajadores deben incluir un aviso al final de cada correo electrónico que aclare que dicho mensaje no vincula a la Empresa X con ningún contrato, posición o acción, a menos que el trabajador esté especialmente autorizado para constituir contratos a nombre de la Empresa X, o autorizado de alguna manera para representar legalmente a la Empresa X.

Comentario: Esta política establece de manera estricta quién puede o no puede comprometer a una organización para que lleve a cabo algún tipo de acción, contrato o adoptar alguna posición. Sin una política como ésta, los correspondentes pueden alegar que un trabajador actuó como si estuviera autorizado a comprometer a la organización y que ellos no tenían motivo para creer que dicho trabajador no estaba autorizado. Los correspondentes pueden alegar que confiaron en el correo electrónico y que ejercieron acciones que los perjudicaron y que ahora la Empresa X debe cumplir lo convenido. Esta política evita tales conflictos y los malos entendidos, sin limitar las actividades comerciales normales. Por ejemplo, el personal de ventas puede negociar los términos de precio y de envío, mientras que el grupo comprador puede comprometer a la organización por ciertos bienes y servicios.

Políticas Relacionadas: “[Contratos Obligatorios en Sistemas Electrónicos](#)” y “[Acuerdos de Negocios por Internet](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Aceptación de Transacciones Computarizadas

Política: Una transacción a ser procesada automáticamente no debe ser aceptada o procesada si no se ha demostrado que el mensaje tiene similitud con el perfil de intercambio de la organización en cuestión, o después de que se haya comprobado la fidelidad y autenticidad de cualquier mensaje que se desvíe del perfil normal de intercambio.

Comentario: Esta política garantiza que no se procesarán automáticamente los mensajes poco comunes sin ser investigados a profundidad. Si un espía activo entrara en un sistema de intercambio de datos electrónicos (EDI, por sus siglas en inglés) y asumiera la identidad de uno de los participantes, los demás participantes podrían seguir las instrucciones recibidas sin verificar su procedencia. Este tipo de problema se puede evitar con el procedimiento general que se define en esta

política. El control de la fidelidad de los mensajes puede incluir una comunicación con un supuesto remitente en particular, a través de un método diferente al del sistema EDI, el cual manejó el mensaje original. Las palabras "perfil de intercambio" se refieren al modo en que un tercero interactúa normalmente con la Empresa X o a las redes que normalmente utilizan los terceros, a la forma en que los mensajes de los terceros están estructurados o a la frecuencia de sus mensajes. La definición de un perfil de cliente se está tomando cada vez más en cuenta en el software de detección de intrusiones. Esta política está redactada para redes inter-organizacionales, pero se puede aplicar a los sistemas intra-organizacionales.

Políticas Relacionadas: “[Contenido de Registros en Aplicaciones de Producción](#),” “[Ofertas y Aceptaciones Electrónicas](#),” “[Ordenes para Cambiar Registros](#),” y “[Autorización para Transacciones en Sistema de Producción](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

16. Ofertas y Aceptaciones Electrónicas

Política: Todos los contratos constituidos a través de mensajes electrónicos de oferta y aceptación se deben formalizar y confirmar a través de documentos en papel, dentro de las dos semanas siguientes a la aceptación.

Comentario: La confirmación a través de un canal de comunicación diferente detecta la presencia de fraude y también valida los acuerdos desde el punto de vista legal. Esta política exige que los usuarios utilicen siempre múltiples canales de comunicación para cada contrato. A medida que crezca la fuerza de las firmas digitales y los códigos de autentificación de mensajes, esta política se tornará innecesaria. Esto se debe a que los controles incluidos en los sistemas computarizados garantizarán en mayor medida que el contrato es legítimo, que proviene de un tercero que supuestamente lo envió y que no ha sido modificado en tránsito. Esta política es una práctica comercial común en el área de compras, donde inicialmente una orden de compra se lleva a cabo telefónicamente y se transmite simultáneamente a través del correo o de un fax.

Políticas Relacionadas: “[Aceptación de Transacciones Computarizadas](#)” y “[Autentificación del Usuario por el Sistema Operativo](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

17. Registros de Telemarcadeo

Política: Los representantes de ventas de la Empresa X deben mantener los registros de los clientes potenciales que hayan expresado a la empresa su deseo de no recibir llamadas relacionadas con ventas.

Comentario: Esta política está dirigida a evitar que algunos clientes potenciales reciban llamadas de telemarcadeo de la Empresa X, si han notificado con anterioridad su deseo de no recibir tales llamadas. La política impedirá de manera directa los inconvenientes de relaciones públicas, mediante la prohibición de llamadas que podrían llevar a litigios incómodos, a editoriales de periódicos y a un boicot por parte de los consumidores. La política también se aplica a los sistemas de llamadas automáticas, los cuales manejan llamadas a través de mensajes pregrabados.

Políticas Relacionadas: "Acoso Sexual, Etnico y Racial" y "Comunicaciones Potencialmente Ofensivas"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

18. Cifrado de Información de Pagos

Política: Toda información sobre compensación, tal como los números de cuentas corrientes y los números de tarjetas de crédito, debe estar cifrada al ser almacenada en cualquier computador de la Empresa X accesible desde Internet.

Comentario: Esta política garantiza que la información sobre compensación no será revelada a hackers, espías industriales, ex-empleados descontentos y terceros no autorizados, en caso de que estos terceros fueran capaces de vencer los sistemas de control de acceso de los computadores accesibles desde Internet. La divulgación de la información es un problema respecto de estos parámetros de compensación, dado que son equivalentes a una contraseña fija. El acceso a los parámetros permite a las personas no autorizadas obtener dinero. Esta política proporciona un segundo nivel de seguridad que sería efectivo aunque los cortafuegos y los controles de acceso basados en contraseñas estén comprometidos. La política evita hacer referencia al tipo de archivo en el cual está ubicada la información sobre compensación, para poder hacerla aplicable a todos los demás archivos. Esta política es una recomendación normal que proviene de las principales compañías de tarjetas de crédito, pero muchos comerciantes en Internet no siguen dicha regla. Esta política hace referencia a los "computadores accesibles desde Internet", no sólo a los "computadores

con conexión a Internet". Esto significa que la política se aplica a todas las máquinas a las que pueda acceder un intruso a través de Internet, no sólo a los computadores que se encuentren en la periferia con interfaces directas hacia Internet.

Políticas Relacionadas: "Acceso a la Información Personal," "Remoción de Registros de Computadores Accesibles desde Internet," y "Eliminación de la Información de Pago"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

19. Confirmación de Información de Pago

Política: Cuando los clientes confirman el uso de una tarjeta de crédito específica, de un número de cuenta corriente o de otra información de pago archivada en la Empresa X, los representantes de la misma deben compartir sólo los últimos dígitos de esta información.

Comentario: Esta política evita el fraude. Si alguien contacta al departamento de ayuda al cliente y confirma un número de tarjeta de crédito almacenado en los sistemas informáticos administrados por la organización, los representantes de ayuda al cliente deberían suministrar sólo los últimos cuatro dígitos. En una aplicación comercial de Internet, si el cliente necesita confirmar el uso de una tarjeta de crédito en particular, sólo se visualizan los últimos cuatro dígitos. Debido a que no se visualiza todo el conjunto de números, los impostores no pueden obtener esta información de pago ni utilizarla para objetivos no autorizados. El usuario autorizado contará con información suficiente para poder confirmar que necesita utilizar ese método de pago en particular. Los dígitos menos significativos de la información de pago se utilizan porque son los que tienen más tendencia a ser modificados de cliente a cliente y de cuenta a cuenta. Si un impostor tuviera que determinar que un individuo sostuvo una relación con una empresa de tarjetas de crédito en particular, los primeros cuatro números serían predeterminados ya que éstos se aplican para todos los clientes y resultarían inadecuados para identificar en forma única un número de tarjeta de crédito. Esta política se aplica cuando cambia la información de pago, como cuando se vence una tarjeta de crédito.

Políticas Relacionadas: "Esconder Transmisión de la Información," "Ordenes para Cambiar Registros," e "Intercambio de Información por Internet"

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos

20. Cifrado de Datos de Pago

Política: La información relacionada con pagos, tal como los números de tarjetas de crédito o los números de cuentas corrientes, debe estar cifrada cuando resida en el computador y también cuando no esté activa para propósitos comerciales autorizados, cuando sea transmitida en redes públicas y cuando esté almacenada en discos o cintas.

Comentario: Esta política impide que los números de tarjetas de crédito y los números de las cuentas corrientes caigan en las manos equivocadas. Para ambos tipos de números, la simple posesión es suficiente para comenzar una transferencia fraudulenta de fondos. Esto se debe a que los números son básicamente contraseñas fijas que autorizan la transferencia de fondos. El cifrado evita que las versiones legibles de estos parámetros sean accesibles a terceros no autorizados. Por ejemplo, si los parámetros están cifrados en el momento de su almacenamiento en una cinta de respaldo, esto impedirá que se puedan cometer fraudes con dichos parámetros, aunque la cinta esté almacenada en un sitio remoto sin controles de acceso físico resistentes. Esta política es consistente con las regulaciones impuestas por las organizaciones emisoras y procesadoras de las principales tarjetas de crédito, y es especialmente importante para aquellas organizaciones que mantienen operaciones comerciales en Internet.

Políticas Relacionadas:“[Cifrado de Correo Electrónico](#)” e “[Identificadores Personales en Ubicaciones Públicas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

21. Números de Tarjeta de Crédito Inactivos

Política: Los números de tarjetas de crédito que no hayan sido utilizadas por más de un año, deben ser eliminados inmediatamente de los sistemas comerciales en Internet.

Comentario: Esta política garantiza que la entrada forzada a un sistema comercial de Internet de un comerciante, no revelará los números de tarjetas de crédito de aquellos clientes que no mantienen una relación comercial con dichos comerciantes. Esta política funciona más efectivamente en combinación con otras políticas, tales como aquéllas que exigen que los números de las tarjetas de crédito estén cifrados en el

momento de su almacenamiento en los sistemas comerciales en Internet y posiblemente con rutinas de sobreescritura para garantizar que estos números eliminados no pueden ser recuperados con utilidades de reparación de discos. La política no compromete el bienestar de los clientes activos, pero sí el de los clientes que no han realizado compras por más de un año.

Políticas Relacionadas:“[Remoción de Registros de Computadores Accesibles desde Internet](#)” y “[Acceso a la Información Personal](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

22. Cuentas Involucradas en Fraudes

Política: Cualquier cuenta financiera con la Empresa X que demuestre la existencia de fraude, debe ser cerrada inmediatamente.

Comentario: Esta política evita fraudes adicionales a los ya existentes. La política puede ser adoptada por cualquier organización que mantenga cuentas financieras con varias organizaciones, inclusive bancos, empresas de crédito y empresas de tarjetas de crédito. La política también puede ser adoptada por organizaciones que ofrecen cuentas financieras, tales como los bancos que funcionan sólo a través de Internet. Si existe un fraude en una cuenta, quiere decir que el impostor está familiarizado con el número de cuenta así como con los demás detalles necesarios para cometer fraude. Si el impostor cometió fraude una vez, puede repetirlo, especialmente si el fraude no ha sido detectado. Al cerrar una cuenta, la organización que adopta esta política impide este tipo de fraude en la misma cuenta.

Políticas Relacionadas:“[Confirmación de Información de Pago](#)” y “[Números de Cuenta Bancaria](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

23. Canal de Confirmación

Política: Todas las transacciones iniciadas a través de Internet, por vía telefónica o por cualquier otro sistema electrónico, deben ser confirmadas inmediatamente por un canal de comunicación alternativo.

Comentario: Debido a que las órdenes de compra se pueden colocar utilizando los números de las tarjetas de crédito, los números de las licencias de conducir y el identificador de usuario robados, se recomienda que los

comerciantes y los otros proveedores de servicio confirmen siempre cada transacción. En este contexto, una transacción podría incluir un cambio de dirección así como también transacciones más usuales, como la compra de bienes. Para un cambio de dirección, muchos bancos enviarán una confirmación a la dirección anterior. Si el cambio de dirección formó parte de un fraude, será detectado por el cliente y él mismo notificará al banco. Asimismo, cuando las órdenes son enviadas a través de una actividad de comercio en Internet, la confirmación de que una orden fue colocada se realiza a través de un correo electrónico. Dicha confirmación debe ser enviada a través de un canal diferente al utilizado para iniciar el pedido, ya que si es colocada a través del mismo canal, simplemente se devolvería al autor potencial del fraude.

Políticas Relacionadas:“Ofertas y Aceptaciones Electrónicas” y “Validación de la Identidad de Terceros”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

24. Saldo y Conciliación de Cuentas

Política: Se deben balancear y conciliar diariamente los registros contables que reflejen las actividades de los sistemas comerciales de pago en Internet.

Comentario:Esta política exige que los registros contables estén vigentes, y que sean precisos y de utilidad para la detección temprana de fallas y fraudes. Debido a que todo es muy rápido en el área comercial en Internet, es primordial que estas actividades se lleven a cabo diariamente o con mayor frecuencia. Estas actividades le permiten a la gerencia realizar otras pruebas en los registros contables, tales como análisis de saldos y de proporciones. Estas actividades se pueden automatizar.

8.07.04 Seguridad de Correo Electrónico

1. Revisión de Mensajes de Correo Electrónico de Terceros

Política: Los trabajadores de la Empresa X pueden leer los mensajes enviados a través de los sistemas de correos electrónicos de la Empresa X que permiten el acceso a terceros, sólo si tanto el remitente como el receptor lo han autorizado.

Políticas Relacionadas:“Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

25. Activación de Tarjeta de Pago

Política: Los mecanismos de pago, tales como las tarjetas de crédito, deben ser activados sólo después de que el receptor correspondiente acuse recibo a través de la provisión de información que sólo él puede dar.

Comentario:Esta política evita los fraudes a través de un mecanismo de pago, tales como una tarjeta inteligente, una tarjeta de debito o una tarjeta de crédito. Debido a que estos mecanismos de pago son enviados con frecuencia a través del correo normal, a menudo se requieren mecanismos mediante los cuales el receptor autorizado pueda informar a la organización emisora que lo ha recibido. Para las tarjetas de crédito, esto se puede realizar a través de llamadas telefónicas gratuitas, en las que los receptores autorizados suministran los últimos cuatro dígitos de su número de seguridad social o alguna otra información personal. Despues de un cierto período de tiempo, si el receptor no ha acusado recibo, se asume que la tarjeta se extravió o fue robada, punto en el cual la tarjeta previamente emitida se puede desactivar y se debe emitir una nueva tarjeta.

Políticas Relacionadas:“Tarjetas de Contraseñas Dinámicas” y “Canal de Confirmación”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

Comentario:Es importante especificar cuándo se pueden leer los correos electrónicos. Esto se convierte en un problema específico cuando una organización alberga a terceros dentro de su red y tiende a parecerse a una operadora telefónica común. Las operadoras comunes tienen algunas obligaciones que no se aplican a las redes privadas. Los usuarios de los sistemas de redes comunes pueden gozar de ciertos derechos legales que no disfrutan los usuarios de redes privadas. Esta política especifica cuándo se permite a los empleados de

la Empresa X examinar correos electrónicos que puedan contener datos confidenciales o personales relacionados con terceros. La política hace referencia a un problema secundario de difusión de la información, en donde un receptor transmite un mensaje a otra persona, y esta persona lo transmite a un tercero al cual el receptor original nunca tuvo la intención de acceder. Los derechos de acceso pueden diferir si una red proporciona acceso al público versus si proporciona acceso sólo a terceros relacionados con las actividades del negocio. Se recomienda consultar al asesor legal interno respecto de políticas como ésta.

Políticas Relacionadas: “[Privacidad en Correo Electrónico](#)” y “[Monitoreo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Información Secreta en Correo Electrónico

Política: La información secreta no cifrada no debe ser enviada a través de correos electrónicos, salvo que un vicepresidente lo autorice específicamente cada vez.

Comentario: El objetivo de esta política es comunicar a los usuarios que no deben confiar en los sistemas de correo electrónico para transmitir información secreta. Los correos electrónicos no cifrados pueden ser interceptados fácilmente por terceros no autorizados. La política no permite una autorización total por parte de un vicepresidente. Si un usuario necesita enviar correos electrónicos con cierta frecuencia, se deberían utilizar facilidades de cifrado u otros medios de transmisión. Esta política es especialmente importante para la Internet, los servicios externos de correos electrónicos y las redes externas con valor agregado.

Políticas Relacionadas: “[Cifrado de Correo Electrónico](#),” “[Entrega de Información Secreta](#),” “[Envío de Información Secreta Vía Fax — Cifrado](#),” “[Seguridad de la Información Sensible](#),” y “[Algoritmo de Cifrado Normal e Implantación](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

3. Direcciones de Correo Electrónico

Política: Los trabajadores no deben utilizar direcciones de ningún correo electrónico distintas a las direcciones de los correos electrónicos oficiales de la Empresa X, para todos los asuntos relacionados con la empresa.

Comentario: Esta política impide que los trabajadores utilicen servicios gratuitos de correos electrónicos y cuentas personales de Internet en asuntos relacionados con la empresa. Algunos empleados pueden utilizar estos servicios externos debido a que de esta manera pueden eludir los controles que la organización ha puesto en práctica para los correos electrónicos oficiales. El uso de direcciones externas puede permitir la entrada de anexos contaminados con virus en la red interna. Esta política muestra una imagen profesional y organizada a los clientes y a los terceros. Con la política también se intenta evitar la confusión en cuanto al uso personal de los sistemas informáticos de la empresa. Si los trabajadores envían mensajes relacionados con el negocio a través de sus cuentas personales y envían mensajes personales a través de sus cuentas comerciales, será difícil diferenciar si el trabajador utilizó en forma excesiva los sistemas informáticos del negocio para propósitos personales. En algunas organizaciones, esta política puede necesitar una condición adicional, que permitiría el uso de tales direcciones externas en caso de emergencia o siniestro.

Políticas Relacionadas: “[Cuentas Unicas de Correo Electrónico](#)” y “[Reenvío Externo de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Información de Contacto del Remitente

Política: Todo correo electrónico enviado utilizando los sistemas informáticos de la Empresa X debe incluir el primer nombre y el apellido del remitente, el título de su cargo, la unidad organizacional y el número telefónico.

Comentario: Esta política exige que todo aquel que utilice los sistemas informáticos de la Empresa X incluya una serie de detalles normalizados con información del remitente en todos los correos electrónicos. Esta política evita confusiones en aquellos casos en los cuales los mensajes han sido reenviados o parte de éstos han sido incluidos en otros mensajes. La política también resulta útil porque exige que todos los remitentes de correos electrónicos se identifiquen, aunque estos correos pasen a través de un reenviador que reenvía los mensajes y borra la identidad del remitente. Esta política también ataca los correos electrónicos anónimos, los cuales pueden ser denigrantes por naturaleza. Algunas organizaciones pueden ampliar esta política para incluir excepciones legales o notificaciones de monitoreo y almacenamiento de mensajes.

Políticas Relacionadas: “Identificadores de Usuarios Anónimos” y “Cuentas Únicas de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Fuente de Material de Mercadeo por Correo Electrónico

Política: Todos los materiales de mercadeo enviados a través del correo electrónico deben incluir una dirección de correspondencia real y deben proporcionar instrucciones claras y precisas que permitan a los receptores su rápida eliminación de la lista de distribución.

Comentario: Esta política prohíbe a los trabajadores de la Empresa X el envío intencional de correos electrónicos orientados al mercadeo con direcciones de correspondencia incorrectas, para no ser molestados por receptores que las objetan al recibirlas. Esta política notifica que la Empresa X siempre indicará el proceso de eliminación asociado a una lista de distribución. La política implica también que el personal de la Empresa X eliminará los nombres y los enlaces personales de una lista de distribución de correos electrónicos, aun cuando la lista esté en manos de terceros y dicha lista esté rentada por la Empresa X. Esta política apoyará a la Empresa X en sus esfuerzos de cumplir las políticas de privacidad de algunos países.

Políticas Relacionadas: “Remoción de Individuos de la Base de Datos” y “Atribución de la Información”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Reenvío Externo de Correo Electrónico

Política: A menos que el Propietario o el generador de la información esté de acuerdo con anterioridad o que la información sea claramente de naturaleza pública, los trabajadores no deben reenviar correos electrónicos a ninguna dirección fuera de la red de la Empresa X.

Comentario: Esta política garantiza que la información confidencial no será reenviada a terceros no autorizados. Esto podría suceder cuando un memorando interno es accidentalmente reenviado a un socio o a una organización externa. Puede que el trabajador no lo piense en el momento, pero la información confidencial podría ser revelada en el proceso de reenvío. Si bien es cierto que estos mecanismos automatizados de reenvío pueden proporcionar a un empleado una forma expedita de

mantenerse al día con sus contactos personales y socios, tales arreglos arriesgan la exposición accidental de la información confidencial.

Políticas Relacionadas: “Manejo de Despidos” y “Revisión de Mensajes de Correo Electrónico de Terceros”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

7. Mensajes de Correo Electrónico Inadecuados

Política: Los trabajadores no deben generar ni enviar o reenviar correos electrónicos que provengan de terceros y que se puedan considerar como acoso o que puedan contribuir a un ambiente hostil de trabajo.

Comentario: Esta política notifica a los trabajadores que no deben generar o reenviar ningún material que pudiera generar un ambiente hostil de trabajo. Aunque los usuarios se puedan resistir a utilizar esta política, es un paso importante para evitar responsabilidades sobre la discriminación en la contratación, el acoso sexual u otros problemas.

Políticas Relacionadas: “Archivo de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

8. Manejo de Mensajes de Correo Electrónico

Política: Los administradores de los sistemas de la Empresa X deben establecer y mantener un proceso sistemático para la grabación, retención y destrucción de correos electrónicos y de los registros que los acompañan.

Comentario: Los correos electrónicos proporcionan una forma efectiva de llevar una cronología de las comunicaciones dentro de la organización y también entre organizaciones. Los correos electrónicos y los registros a menudo son vistos como parte de los procedimientos que acompañan a un litigio. Esta política exige que se implante un proceso normalizado de manejo de mensajes y registros. En algunas instancias, los correos electrónicos y los registros deben ser conservados más allá de los períodos normales de retención. Aunque posiblemente no se amplíe su alcance, esta política puede aplicarse igualmente al correo de voz.

Políticas Relacionadas: “Cronograma de Retención de los Archivos Almacenados” y “Revisión de la Información Respaldada”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Retención de Mensajes de Correo Electrónico

Política: Un correo electrónico debe ser conservado como referencia futura si contiene información importante para la culminación de una transacción comercial, si contiene información de referencia potencialmente importante o si tiene valor como evidencia para una decisión gerencial de la Empresa X.

Comentario: Esta política evita la destrucción inapropiada de información valiosa. Muchos usuarios no tienen la seguridad de cuáles correos electrónicos deben ser retenidos y cuáles deben ser eliminados después de su recepción. Muchas organizaciones podrían modificar la descripción de los mensajes que deben ser conservados. Una definición explícita de “transacción comercial” puede servir de apoyo a los lectores de esta política.

Políticas Relacionadas: “Manejo de Mensajes de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Almacenamiento de Mensajes de Correo Electrónico

Política: Los usuarios deben guardar regularmente la información importante, convirtiendo los archivos de mensaje de correo electrónico a documentos de procesadores de palabras, bases de datos y otros archivos.

Comentario: Esta política está dirigida a lo que se ha convertido en un mal hábito de muchos usuarios. Abrumados por el volumen de comunicaciones que reciben, los usuarios simplemente guardan ciertos mensajes de correo electrónico. Desafortunadamente asumen que el mensaje guardado estará disponible cuando lo requieran más tarde, pero muchos sistemas de correo no han sido diseñados como bases de datos y no tienen mecanismos adecuados para proteger la información importante. Un problema de corrupción de datos en el disco duro podría causar la pérdida total del buzón de correo electrónico. Esta política intenta preservar información importante, especialmente aquella enviada como anexo de mensaje electrónico. Tal como ocurre con el respaldo de los datos personales, los usuarios toman en serio esta materia sólo tras la pérdida de material importante.

Políticas Relacionadas: “Manejo de Mensajes de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Destrucción de Mensajes de Correo Electrónico

Política: Todos los mensajes de correo electrónico multiusuario deben destruirse al cumplirse un año desde el momento en que fueron archivados.

Comentario: Esta política está orientada a minimizar el volumen de mensajes de correo electrónico archivados, al conservar espacio de disco y simplificar las actividades de manejo de la información. Desde el punto de vista legal, esta política está orientada a evitar que una organización se encuentre en una difícil situación porque la gerencia cree haber borrado todos los registros pertinentes a un asunto, cuando todavía tiene correo electrónico archivado. Muchos abogados usan el correo electrónico como una fuente de información que esperan se convierta en evidencia al descubrirla. Cuando una política como ésta existe en una organización, no puede ser acusada de destrucción deliberada de evidencias, puesto que dicha destrucción es parte de un procedimiento administrativo ordinario. Es aconsejable una aclaratoria que informe a los usuarios finales cuál

tipo de información retener y por cuánto tiempo. Aunque esta política se aplica a servidores de archivo y otros sistemas multiusuario, se podría extender a los computadores personales. El periodo de tiempo de archivo pudiera acortarse de un año a tres meses.

Políticas Relacionadas: “Destrucción de Información Sensible” y “Moratoria en Destrucción de Datos”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

12. Privacidad en Correo Electrónico

Política: El correo electrónico es información privada y se debe manejar como comunicación privada y directa entre un remitente y un receptor.

Comentario: Esta política claramente especifica qué tipo de privacidad deberían esperar los trabajadores en cuanto al correo electrónico. Un claro entendimiento del nivel de privacidad que disfrutan, permitirá a los usuarios tomar decisiones apropiadas sobre el tipo de información a enviar mediante correo electrónico. Esta política es intencionalmente vaga acerca de aspectos tales como la lectura de mensajes para permitir la administración de un sistema de correo electrónico. Esta revisión de mensajes sería parte de esta política, siempre y cuando la intención fuese mantener y administrar el sistema y no violar la privacidad de alguien. Si la gerencia desea usar el sistema de correo electrónico para monitorear el rendimiento del trabajador, descubrir conductas no éticas y asegurar el uso apropiado del sistema, la política se puede expandir con el fin de incluir frases tales como "el correo electrónico se revisará rutinariamente para descubrir conductas poco éticas". Esta política se puede extender igualmente para incluir acciones específicas tales como "el correo electrónico no debe ser monitoreado, visualizado, reproducido o de modo alguno usado por ninguna otra persona que no sean el remitente y el receptor". Esta política también se puede expandir y aplicar a mensajes de correo de voz.

Políticas Relacionadas: “Privacidad del Archivo Personal,” “Monitoreo de Mensajes de Correo Electrónico,” y “Revisión de Mensajes de Correo Electrónico de Terceros”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

13. Cifrado de Correo Electrónico del Cliente

Política: Se deben cifrar todos los mensajes de correo electrónico que contengan información acerca de uno o más clientes específicos.

Comentario: Esta política preserva la privacidad de clientes preocupados por la intercepción no autorizada de su correo electrónico. La política también previene fraudes como el robo de identidad al evitar que personas no autorizadas obtengan acceso a la información privada. El alcance de la política se puede expandir con la finalidad de incluir clientes potenciales además de los clientes actuales, pero los clientes potenciales pudieran no tener el software necesario para respaldar las comunicaciones codificadas. Esta política se puede poner en práctica en algunos sitios web mediante una función especial para enviar un mensaje a los proveedores, y esta función especial típicamente transmite un mensaje en forma codificada. La política también se puede poner en práctica mediante software de cifrado y las facilidades de cifrado incluidas en ciertos sistemas de correo electrónico. La política es bidireccional porque se aplica tanto a las comunicaciones desde un cliente hacia la Empresa X, como desde la Empresa X hacia un cliente.

Políticas Relacionadas: “Información Secreta en Correo Electrónico” y “Privacidad en Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

14. Cifrado de Correo Electrónico

Política: Toda información sensible, incluyendo, sin limitantes, los números de las tarjetas de crédito, las contraseñas y la información de investigación y desarrollo, debe estar cifrada para su transmisión vía correo electrónico.

Comentario: Esta política informa a los usuarios que sus comunicaciones de correo electrónico no están protegidas de la misma manera que el servicio postal protege una carta ordinaria. La política notifica a los usuarios que la información sensible no se debe enviar por Internet a menos que esté cifrada. Es común que los analistas de redes capturen y almacenen información que pasa por enlaces de Internet, lo cual se puede hacer de mala fe con igual facilidad. Esta política se puede modificar para que haga referencia a "Internet y otros sistemas de correo electrónico externo" en lugar de simplemente "correo electrónico". Esto permitiría que los sistemas de correo electrónico internos manejen

información sensible, mientras que los trabajadores no deben usar sistemas de correo electrónico externo para información sensible. La política asume que la palabra "sensible" ya está definida.

Políticas Relacionadas: "Información Secreta en Correo Electrónico," "Clasificación de Datos en Cuatro Categorías," "Cifrado de Contraseñas," y "Envío de Información Secreta Vía Fax — Cifrado"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Autorización para Monitorear Mensajes de Correo Electrónico

Política: Los trabajadores no deben monitorear sistemas de correo electrónico en cumplimiento de políticas internas, por sospecha de actividad delictual y otras razones administrativas de la gerencia de sistemas, a menos que las tareas de monitoreo del correo electrónico hayan sido delegadas y aprobadas por los directores de Servicios Informáticos y Recursos Humanos.

Comentario: Esta política determina quién puede leer mensajes de correo electrónico y las circunstancias exactas de cuándo los mensajes se pueden examinar. La política notifica implícitamente a los trabajadores que su correo electrónico puede ser monitoreado, lo cual es un paso importante en establecer las expectativas de estos usuarios. Se aconseja consultar las leyes locales acerca del monitoreo de mensajes de correo electrónico para

obtener información adicional al redactar esta política. Algunas organizaciones podrían reemplazar las palabras "otras razones administrativas" con palabras como "supervisión, control y operación eficiente del lugar de trabajo".

Políticas Relacionadas: "Monitoreo de Mensajes de Correo Electrónico"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

16. Modificación de Correo Electrónico

Política: Los trabajadores no deben modificar, falsificar o eliminar cualquier información que aparezca en cualquier lugar de un mensaje de correo electrónico, incluyendo el cuerpo del mensaje o el encabezado.

Comentario: Esta política notifica a los usuarios que no deben jugar con el sistema de correo electrónico, que éste sólo se debe utilizar para actividades del negocio y siempre de manera eficiente. Esta política es necesaria, ya que es sumamente fácil modificar un mensaje de correo electrónico sin que se detecte su modificación por parte del receptor, a menos que el remitente utilice cifrado o una firma digital.

Políticas Relacionadas: "Sitios Web y Comerciales en Internet" y "Cuentas Únicas de Correo Electrónico"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

17. Contenido de Mensaje de Correo Electrónico

Política: Los trabajadores no deben usar lenguaje obsceno, groserías o comentarios despectivos en mensajes de correo electrónico en relación con empleados, clientes o competidores.

Comentario: Muchos usuarios consideran que el correo electrónico es más informal que las tradicionales cartas en papel. La intención de esta política es informar a los trabajadores que son responsables del contenido de sus mensajes y que un contenido inapropiado se puede convertir en un problema legal para su patrono. Esta política también indirectamente combate la práctica de desahogar emociones negativas mediante el correo electrónico. Algunas organizaciones pudieran ampliar la política con el fin de mencionar acoso, molestia, indecencia, intimidación o alguna otra implicación de carácter no ético, inmoral o ilícito.

Políticas Relacionadas: “[Excepción de Responsabilidad en Mensajes Personales en Internet](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Restricciones en Contenido de Mensajes

Política: Los trabajadores no deben enviar o remitir ningún mensaje a través de los sistemas informáticos de la Empresa X que pueda ser considerado difamatorio, hostigante o de naturaleza explícitamente sexual u ofensiva a persona alguna sobre la base de raza, sexo, origen, orientación sexual, religión, creencias políticas o discapacidad física.

Comentario: Esta política protege a la Empresa X contra una variedad de litigios que incluyen difamación, libelo, acoso sexual y la creación de un ambiente de trabajo hostil. Esta política notifica a los trabajadores que los sistemas informáticos de la Empresa X no se deben utilizar para el ejercicio de su derecho a la libre expresión. Una política como ésta debe estar acompañada por otra política que restrinja el uso del sistema de información de la Empresa X a las actividades del negocio.

Políticas Relacionadas: “[Sin Responsabilidad en Mensajes](#)” y “[Uso Personal de los Sistemas de Computación y de Comunicaciones](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Monitoreo de Contenido de Correo Electrónico

Política: Los trabajadores deben limitar sus comunicaciones a asuntos de negocios, reconociendo que la Empresa X emplea de manera rutinaria herramientas de revisión del contenido del correo electrónico para identificar ciertas palabras claves, tipos de archivo y otros tipos de información.

Comentario: El objetivo de esta política es dar a conocer a los usuarios que sus mensajes de correo electrónico serán automáticamente revisados en busca de ciertos tipos de palabras y archivos. La política se hace deliberadamente vaga al describir la naturaleza exacta de la revisión y permitir que estas facilidades se puedan actualizar sin avisar a la comunidad de usuarios. La naturaleza vaga de la política es también deseable porque genera dudas en la mente de los usuarios, lo cual funciona en contra de las transmisiones de correo electrónico ilegales o inadecuadas. Siempre se debe obtener asesoría legal en referencia a todos los aspectos relacionados con el monitoreo de empleados, dada su naturaleza confidencial. El monitoreo aquí mencionado es a menudo puesto en práctica a nivel del cortafuego o a nivel del servidor de correo, para poder detectar y bloquear el flujo saliente de información sensible.

Políticas Relacionadas: “[Responsabilidad de Monitorear Contenido](#)” y “[Sin Responsabilidad en Mensajes](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

20. Mensajes Personales No Solicitados de Correo Electrónico

Política: Los trabajadores que usen los sistemas informáticos de la Empresa X deben suspender inmediatamente el envío de mensajes personales de correo electrónico a todo destinatario que solicite el cese de tal práctica.

Comentario: Esta política evita problemas judiciales tales como alegatos de acoso sexual o la creación de un ambiente hostil de trabajo. Esta política también impide que los trabajadores molesten a clientes potenciales o clientes que han solicitado que no se les contacte. En caso extremo de acoso, el receptor pudiera alegar que su privacidad ha sido violada. Como lineamiento general de negocios, es sabio acatar prontamente las solicitudes de terceros en el sentido de no contactarlos más.

Políticas Relacionadas:“[Acoso Sexual, Etnico y Racial](#)” y “[Contenido de Mensaje de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

21. Correo Electrónico en Volumen

Política: Los trabajadores no deben utilizar los computadores de la Empresa X para la transmisión masiva de ningún tipo de anuncios de correo electrónico no solicitados, o de mensajes comerciales que pudieran iniciar quejas de sus receptores.

Comentario: Esta política impide que los usuarios abusen de la conectividad a la red de los sistemas de correo electrónico, al permitirles alcanzar un gran número de personas a bajo costo. La política reduce las quejas de los clientes y los costos en que se incurría al resolver dichas quejas. La política aclara que la Empresa X no permite ni emplea correo electrónico masivo y de suceder, sería una decisión individual. La política también permite que una organización despida al trabajador que envíe correo electrónico masivo utilizando las facilidades del sistema de la Empresa X. La política podría incluir una medida de prohibición de recopilación de respuestas originadas por dichas transmisiones masivas no solicitadas.

Políticas Relacionadas:“[Remoción de Individuos de la Base de Datos](#)” y “[Fuente de Material de Mercadeo por Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

22. Respuesta a Correo Electrónico No Solicitado

Política: Cuando los trabajadores reciban correo electrónico no solicitado y no deseado, deben remitir el mensaje al administrador de correo electrónico y no responder al remitente de manera directa.

Comentario: Esta política garantiza que los sistemas de correo electrónico interno se usarán exclusivamente para asuntos de negocio y sólo por trabajadores autorizados. El correo electrónico no solicitado crea una merma de la productividad del trabajador y una degradación en la disponibilidad del sistema por congestionamiento en la red y de los buzones de correo electrónico entrante. Esta política orienta a los trabajadores en el sentido de no responderlos. En su lugar,

deben remitirlos a un administrador, quien establece filtros a nivel del cortafuegos o al nivel del servidor de correo electrónico para evitar que dichos mensajes alcancen los buzones de entrada. Los administradores también pueden notificar esta actividad a varias listas negras en Internet que se usan para bloquear estos mensajes de correo electrónico. Los administradores pueden también contactar al proveedor de servicios de Internet en donde fueron creados los mensajes y solicitar que esa cuenta sea revocada.

Políticas Relacionadas:“[Transmisiones a Través de Correo Electrónico y Correo de Voz](#)” y “[Mensajes de Correo Electrónico Inadecuados](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

23. Envíos de Correos Electrónicos No Solicitados

Política: Los usuarios no deben enviar grandes cantidades de correo electrónico no solicitado a ninguna dirección en ninguna red.

Comentario: Esta política informa a los usuarios que no se puede aceptar el envío de grandes cantidades de correo electrónico a persona alguna. Esta práctica no sólo consume los recursos del computador y de la red innecesariamente, sino que requiere que el receptor dispense un mayor período de tiempo para ordenar todos los mensajes no solicitados. Como resultado de este tipo de ataque, el disco del servidor de correo del receptor puede quedar saturado y requerir la intervención del operador. Mientras algunos programas de correo electrónico pueden filtrar y eliminar mensajes de ciertas direcciones, esta política intenta detener la práctica desde su punto de origen.

Políticas Relacionadas:“[Consumo de Recursos por Programas](#)” y “[Retención de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

24. Revisión de Correo Electrónico y Pies de Página

Política: Todos los servidores de la Empresa X deben revisar cada uno de los mensajes entrantes de correo electrónico con el fin de detectar virus y contenidos personales, agregando a cada mensaje una nota al pie de página que indique que ha sido revisado.

Comentario: Esta política informa a los administradores y diseñadores de sistemas y a otros que configuren y manejen los sistemas de correo electrónico, acerca del requisito de revisar, no sólo con la intención de detectar virus y revisar el contenido, sino por la inclusión de avisos que describan dicha revisión. La inclusión de este aviso también alerta a los usuarios sobre el material que está siendo revisado y que, por lo tanto, no es privado. El pie de página motiva a los usuarios a restringir sus interacciones a través del sistema de correo electrónico, limitándolas a asuntos de negocios. La naturaleza del filtrado de contenido a ser llevado a cabo no se especifica, presionando a los usuarios a que sean cuidadosos cuando revisen los mensajes. Varios proveedores ofrecen programas de revisión que respaldan una política como ésta. El antivirus debe estar también instalado y activado en las máquinas de escritorio.

Políticas Relacionadas: “[Respuesta a Correo Electrónico No Solicitado](#)” y “[Comunicaciones Salientes en Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

25. Pie de Página de Correo Electrónico Saliente

Política: Un pie de página elaborado por el departamento Legal, que indique que el mensaje puede contener información confidencial, que sólo puede ser usado por los receptores mencionados, que ha sido registrado para propósitos de archivos, que puede ser revisado por personal de la Empresa X distinto al indicado en la cabecera del mensaje y que no constituye necesariamente una posición oficial de la Empresa X, debe anexarse automáticamente a todos los correos electrónicos salientes que procedan de los computadores de la Empresa X.

Comentario: Esta política garantiza que los receptores del correo electrónico originado en la Empresa X tendrán conocimiento de la naturaleza legal del mensaje recibido. Esta política está dirigida al personal técnico que configura y maneja los sistemas de correo electrónico. La política describe un pie de página de correo electrónico saliente que es parecido a las palabras legales que a menudo se añaden a las portadas de fax. Típicamente este lenguaje de pie de página incluye frases como “este mensaje está dirigido sólo a los receptores indicados y si es visualizado por otras personas, éstas se consideran notificadas de que el material puede ser de naturaleza confidencial y no debe

ser usado por ningún otro que los receptores nombrados”. Otras frases incluidas en pie de página son que las afirmaciones realizadas en el mensaje pertenecen al generador y no necesariamente reflejan la posición oficial de la Empresa X. El lenguaje específico pudiera cambiar de jurisdicción a jurisdicción.

Políticas Relacionadas: “[Revisión de Correo Electrónico y Pies de Página](#)” y “[Aviso en Cubierta de Fax](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

26. Monitoreo de Mensajes de Correo Electrónico

Política: La Empresa X debe notificar a todos los usuarios que los sistemas de correo electrónico son sólo para propósitos de negocios, que todos los mensajes enviados por correo electrónico son registros de la Empresa X, la cual se reserva el derecho de acceder y divulgar todos los mensajes sin previo aviso a ninguno de los involucrados, y que los supervisores pueden revisar las comunicaciones de correo electrónico de sus supervisados con el fin de determinar si se ha violado la seguridad y la política de la Compañía o si se han llevado a cabo otras actividades no autorizadas.

Comentario: Esta política le da más peso a la capacidad de monitorear el correo electrónico que a los derechos de los trabajadores de comunicarse en privado. Esta política garantiza que los trabajadores son notificados de que sus comunicaciones pueden ser monitoreadas sin su previo consentimiento. Este aviso intenta evitar controversias sobre lo conveniente o no de las acciones de la gerencia al monitorear el tráfico de correo electrónico. Sin embargo, los procedimientos que acompañan a esta política podrían ser frustrados mediante el cifrado del correo electrónico. Para que esta política sea totalmente efectiva, debe estar acompañada con una política adicional que prohíba el cifrado en estos casos.

Políticas Relacionadas: “[Autorización del Proceso de Cifrado — Sistemas](#),” “[Areas de Monitoreo Electrónico](#),” “[Herramientas de Monitoreo de Sistemas](#),” “[Monitoreo de Mensajes de Correo Electrónico](#),” y “[Revisión de Mensajes de Correo Electrónico de Terceros](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

27. Archivo y Revisión de Correo Electrónico

Política: Todo correo electrónico enviado mediante el servidor de correos de la Empresa X debe archivarse y estará sujeto a revisión por otra persona distinta del receptor y el remitente.

Comentario: Esta política garantiza que todos los correos electrónicos enviados a través de una organización en particular serán archivados. El remitente y los receptores se consideran informados en el sentido de que sus comunicaciones no son privadas. Esta política es requerida también por algunas agencias del gobierno preocupadas por posibles tergiversaciones efectuadas para con los clientes. Esta política a menudo se anexa a los correos electrónicos para que todos los remitentes externos sepan que todos sus mensajes serán archivados y revisados.

Políticas Relacionadas: “[Destrucción de Mensajes de Correo Electrónico](#)” y “[Manejo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

28. Correo Electrónico del Departamento de Ventas

Política: Los vendedores no deben enviar mensajes de correo electrónico a los clientes o clientes potenciales, a menos que estos mensajes sean previamente revisados y aprobados por un supervisor.

Comentario: Esta política evita que los vendedores realicen ofertas que puedan dañar la reputación de su patrono, forzar al patrono a honrar un acuerdo que no ha realizado o hacer responsable al patrono por tergiversación. Si, por ejemplo, un corredor de bolsa usara las palabras "ganador seguro" respecto a una oferta de acciones de una compañía, estas palabras podrían ser detectadas mediante un programa de revisión de contenido y posteriormente sujetas a un escrutinio humano adicional. Esta política se puede poner en práctica enviando todos los correos electrónicos salientes desde el departamento de ventas y hacer que uno o más supervisores revisen ciertos mensajes, gastando entonces un tiempo considerable al examinar todos aquellos mensajes que un filtro detectaría como potencialmente problemáticos. La necesidad de esta política surge de la tendencia de los vendedores de hacer grandes esfuerzos por obtener un pedido y a decir cosas que puedan afectar la seguridad

de la información. Esta política prohíbe a los vendedores el uso del servicio de correo electrónico gratuito para eludir los procedimientos incorporados en los sistemas de correo electrónico de la Empresa. Esta política motiva el desarrollo de respuestas tipo patrón para consultas de rutina.

Políticas Relacionadas: “[Archivo y Revisión de Correo Electrónico](#)” y “[Monitoreo de Contenido de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

29. Archivo de Correo Electrónico

Política: Todos los mensajes de correo electrónico oficiales de la Empresa X incluyendo, sin limitantes, aquéllos que contienen una autorización formal de la gerencia o una delegación de responsabilidad o gestión parecida, deben copiarse al departamento de archivo de registros.

Comentario: Esta política reconoce la naturaleza cambiante de la función del archivo de registros en muchas organizaciones. En lugar de un ente de manejo de papel, éstos son cada vez más un grupo de gestión de registros electrónicos. El copiado de tales mensajes de correo electrónico proporciona evidencia e identifica quién debe ser el responsable, de generarse controversias, acciones disciplinarias o procesos judiciales. El proceso de almacenado de una copia oficial de correo electrónico Internet es un servicio anunciado por los sistemas de varias organizaciones. No obstante, se puede establecer un grupo interno para realizar esta misma función con firmas digitales u otra tecnología. Si el contenido del mensaje es sensible, entonces el mensaje se debe cifrar. Esto genera la necesidad de desarrollar y administrar las claves de cifrado. Más que guardar la totalidad del mensaje, en algunos casos puede ser suficiente fraccionar los mensajes, aplicar firmas digitales o extraer la información esencial que se va a almacenar, lo cual permitiría la verificación de una transacción específica, por cierto grupo, por ciertas cantidades, en un momento y fecha determinada, pero no permitiría reconstruir fielmente el mensaje original.

Políticas Relacionadas: “[Manejo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

30. Usos del Sistema de Correo Electrónico

Política: Los trabajadores deben usar esencialmente los sistemas de correo electrónico de la Empresa X para fines del negocio, y cualquier uso personal no debe interferir con las actividades comerciales normales, no debe implicar mensajes insinuantes, no deberá asociarse con ninguna actividad comercial para lucro individual diferente de las actividades normales de trabajo y no deberá colocar a la Empresa X en situaciones potencialmente engorrosas.

Comentario: Esta política especifica lo que está permitido en cuanto al uso personal del sistema de correo electrónico de la compañía. Esta política garantiza que este uso personal se mantendrá dentro de ciertos límites. En algunas organizaciones, la frase "actividad comercial para lucro individual" deberá ser definida.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones,” “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones,” “Uso Personal del Teléfono,” y “Uso Distinto al Empresarial de la Información de la Organización”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

31. Distribuciones de Correo Electrónico

Política: La Empresa X debe recibir confirmación mediante un proceso de auto-registro y validación de cada individuo incluido en una lista de distribución de correo electrónico.

Comentario: Esta política evita quejas y mala publicidad asociadas a correos electrónicos no solicitados y no deseados. En algunas jurisdicciones, esto puede también evitar problemas judiciales. Con esta política, las organizaciones preguntarían a los clientes potenciales y a otros, si desean recibir cierto tipo de información y entonces, sólo si los receptores responden afirmativamente, serían incluidos en una lista de distribución de correo electrónico. El personal de mercadeo puede objetar esta política, indicando que se comprometen indebidamente sus actividades de ventas, sin tomar en cuenta la preservación de la privacidad del individuo.

Políticas Relacionadas: “Servicio Nuevo o Mejorado” y “Autorización para Inclusión en Sistemas de Datos Privados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

32. Firmas en Correo Electrónico

Política: Los trabajadores no deben emplear versiones digitalizadas de sus firmas autógrafas con el fin de dar la impresión de que un mensaje de correo electrónico u otra comunicación electrónica ha sido firmada por el remitente.

Comentario: Esta política restringe la diseminación de firmas autógrafas en forma digital. Si estas firmas digitalizadas llegan a las manos equivocadas, podrían ser usadas para falsificar cheques, autorizar pagos con tarjetas de crédito de manera fraudulenta y obtener tarjetas de identificación de modo inadecuado. No se recomienda duplicar los controles manuales en un entorno automatizado ya que los resultados pueden ser catastróficos. Existen otros controles más confiables para autenticar la identidad de los generadores de mensajes de correos electrónicos. Estos incluyen firmas digitales, certificados digitales, cifrado y sistemas de contraseñas dinámicas.

Políticas Relacionadas: “Originador de Transacciones” y “Validación de la Identidad de Terceros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

33. Anexos de Correo Electrónico

Política: Los trabajadores no deben abrir los anexos de correo electrónico, a menos que provengan de un remitente conocido y confiable o hayan sido revisados por un paquete de software antivirus autorizado.

Comentario: Esta política evita las contaminaciones por virus en computadores de escritorio. Los anexos ejecutables son una vía común para la entrada de virus en una red interna y el daño resultante puede ser significativo y costoso. Muchos de estos virus usan la libreta de direcciones en la aplicación de correo electrónico, para reenviar automáticamente el virus a todas las direcciones allí contenidas. Esas transmisiones serían enviadas desde un remitente conocido, pero como el anexo no está contemplado, se supone que el receptor no lo abrirá. Ciertos anexos, tales como aquéllos en formato RTF son inocuos debido a que ese formato no contiene componentes ejecutables. La política se podría modificar para permitir la apertura de anexos de texto, pero no se podría confiar que los usuarios identifiquen

de manera confiable el tipo de formato de los archivos anexos recibidos. Esta política no evitaria la entrada de virus a la red interna, pero puede ayudar. Otra forma de redactar la política puede ser: "Se puede abrir un anexo si el texto del correo que acompaña al anexo tiene sentido y es congruente con las actividades de negocio actuales y si el anexo fue enviado por un remitente conocido y confiable".

Políticas Relacionadas: "[Descarga de Software](#)" y "[Direcciones de Correo Electrónico](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

34. Anexos Entrantes de Correo Electrónico

Política: Los trabajadores que necesiten recibir desde una fuente externa un archivo con formato, un programa ejecutable o algún otro mensaje no texto, deben usar un método de transmisión diferente al correo electrónico.

Comentario: Esta política evita la transmisión inadvertida por Internet a los computadores de la Empresa X de virus tipo macro vía anexos de correo electrónico. Los virus tipo macro se incorporan a los archivos de datos en lugar de hacerlo a programas ejecutables. Esto también protege parcialmente a la organización contra contenido dinámico, el cual es un riesgo cada vez más fuerte que enfrentan los usuarios de Internet. La política requiere que los usuarios conviertan a formato de texto simple los documentos de procesadores de palabras, hojas electrónicas y otros archivos y los incluyan en el cuerpo de un mensaje de correo electrónico. Esta política reconoce que, además de los discos flexibles, los anexos de correo electrónico han llegado a ser el mecanismo más usado para propagar virus macro. Esta política también minimiza la transmisión de archivos ejecutables, lo que probablemente reduce las contaminaciones de virus ordinarios que se propagan como parte de los archivos ejecutables. Esta política asume que un código especial se ha incluido en los programas de manejo de correo electrónico para realizar la revisión necesaria, ya que resulta mejor aplicar una política de manera automática que depender de los usuarios. Muchos sistemas cortafuegos tienen ahora la capacidad para hacer este tipo de revisión, pero puede estar incompleto o ser no confiable. Esta política puede parecer muy restrictiva para muchas organizaciones.

Políticas Relacionadas: "[Censura de Datos](#)"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Altos

35. Anexos de Correo Electrónico No Esperados

Política: Los usuarios que reciban un anexo no esperado en un mensaje de correo electrónico sin una aclaratoria creíble que indique que se trata de algo pertinente a la relación comercial, no deben abrir el anexo hasta obtener una aclaratoria del remitente.

Comentario: Esta política evita que los usuarios procesen accidentalmente anexos que afecten sus computadores con virus, gusanos y otros elementos destructivos. Al abrir un anexo se puede ocasionar la infección de un computador personal con virus. Esta política no prohíbe a un usuario abrir anexos y no los bloquea en un sistema cortafuego. Los anexos son útiles y a menudo usados, pero al mismo tiempo pueden invocar de manera automática programas que realizan actividades indeseables y dañinas sin el conocimiento o consentimiento del usuario. Se recomienda borrar los anexos para evitar ser abiertos de manera accidental posteriormente. Esta política no sustituye a un programa de detección de virus activo en cada computador del usuario.

Políticas Relacionadas: "[Anexos de Correo Electrónico](#)" y "[Ejecución de Código Móvil](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

36. Foros Electrónicos Públicos

Política: Los trabajadores no deben usar los sistemas informáticos de la Empresa X para participar en grupos de discusión de Internet, salones de charlas u otros foros electrónicos públicos, a menos que esta participación sea expresamente autorizada por el departamento de Relaciones Públicas.

Comentario: Esta política le evita a la Empresa X exponerse a una situación vergonzosa y hasta entrar en litigios. Esta política limita a la representación de la organización en Internet. La política es necesaria ya que muchas personas adoptan una actitud informal respecto al envío de material en Internet. Las palabras "foros electrónicos públicos" podrían incluir teleconferencias en línea y otros arreglos comunicacionales. La redacción es deliberadamente vaga para poder abarcar nuevas tecnologías sin tener que modificar la política.

Políticas Relacionadas: “Aprobación de las Representaciones Públicas,” “Divulgación de Secretos Industriales por Internet,” y “Derecho a la Libre Expresión”

8.07.05 Seguridad de los Sistemas Electrónicos de Oficina

1. Registros de Faxes

Política: Se deben retener por el período de un año los registros de cada transmisión de fax entrante y saliente, incluyendo los números de teléfono pertinentes y el número de páginas de cada transmisión.

Comentario: Esta política provee un registro legal de los faxes que han sido enviados y recibidos. Esto es importante en aquellos entornos donde los contratos de negocio, las órdenes de compra, las facturas y otros documentos legalmente vinculantes se manejan por fax. El mantenimiento y archivo de un registro de faxes pueden ayudar a resolver problemas operacionales del día a día. Tales registros de faxes pueden además ser de gran utilidad en la preparación de cuentas de gastos e informes del sistema de reversión de cargos. Muchos paquetes nuevos de software para computadores personales que respaldan el procesamiento de faxes, vienen con su propio sistema de registros que, por efecto de esta política, debería estar habilitado. Los servidores de fax también soportan sistemas amplios de registro.

Políticas Relacionadas: “Envío de Información Sensible Vía Fax — No Cifrada”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

2. Actualizaciones de Software de Computadores Personales

Política: Los usuarios no deben instalar programas nuevos o actualizados en su estación de trabajo o computador personal, sino que deben depender para este mantenimiento de los administradores del sistema a través de descargas automáticas desde la red.

Comentario: Esta política garantiza que el conjunto de aplicaciones se ejecutará en todas las estaciones de trabajo de una organización. Esto se puede lograr con paquetes de distribución automática de software. La conformidad con esta política puede ser comprobada mediante programas de administración automática de licencias. Un conjunto de aplicaciones, como el antes descrito, es conveniente porque tiene un costo conside-

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

rablemente menor, es más fácil de respaldar y es probablemente más seguro. El software más moderno es cada vez más modular y configurable. Esto implica que ciertas opciones puedan ser deshabilitadas o eliminadas antes de distribuir el software.

Políticas Relacionadas: “Instalación de Software por Usuario”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Programas de Aplicación de Usuarios Finales

Política: Todos los sistemas de menor escala deben usar programas autorizados de administración de licencias que se configuren para detectar copias no autorizadas de software de terceros y programas de aplicación nuevos o modificados desarrollados por usuarios finales.

Comentario: Esta política promueve un entorno de computación informal en que los usuarios finales pueden realizar su propia programación de aplicaciones de sistemas, siempre y cuando éstas no se usen como aplicaciones de producción. La política requiere que se empleen programas de administración de licencias para vigilar esta actividad. Mediante estos programas de administración de licencias, todas las nuevas aplicaciones serán identificadas y, si se demuestra posteriormente que son aplicaciones de producción, se puede exigir al usuario en cuestión que documente la aplicación desarrollada y agregue controles adicionales. En algunos entornos, una pantalla especialmente diseñada puede preguntarle a los desarrolladores en el departamento usuario final, si el software se usa para fines productivos. Si queda demostrado que es software de producción, entonces se le exigirá que cumpla con las normas de desarrollo y de documentación. Esta política apoya la generación de prototipos y una filosofía de desarrollo evolutivo de sistemas. El departamento de Sistemas Informáticos no pierde el control con este mecanismo, porque puede evitar el uso de cualquier software mediante el sistema de administración de licencias. Este paso puede ser el apropiado cuando los

sistemas así desarrollados carezcan de un proceso de verificación apropiado o de su documentación respectiva. Con el software de administración de licencias, Sistemas Informáticos puede también monitorear todos los programas nuevos o modificados en los sistemas conectados en red.

Políticas Relacionadas: “Convenciones en Desarrollo de Sistemas” y “Lenguajes de Programación de Alto Nivel”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Lógica Crítica de Negocios

Política: Las aplicaciones de producción que contengan lógica crítica de negocios, se deben ejecutar en servidores multiusuario que deben tener controles de acceso físico, controles de acceso lógico, controles de cambios y planes de contingencia.

Comentario: Esta política evita que la lógica crítica de negocios esté al alcance de personas no autorizadas si intentaran robar un computador portátil o de escritorio. Desde una perspectiva diferente, mantener los programas de lógica crítica de negocios sólo en máquinas multiusuario mayores, con controles de acceso físico, evita que se diseminen copias de ésta y de esa manera se controla el acceso a los secretos industriales, prácticas de negocio único y otras ideas sensibles. A menudo los sistemas de escritorio y portátiles carecen de controles de cambios y por ende son susceptibles a virus, gusanos y otros problemas que los sistemas multiusuario con controles de acceso generalmente no lo son. Los sistemas portátiles y de escritorio también carecen a menudo de contraseñas, cifrados y otros controles de acceso lógicos para prevenir la divulgación de la información manejada por estas aplicaciones críticas. Los sistemas de escritorio y portátiles también pueden ser no ideales para aplicaciones de producción porque puede ser fácil para los usuarios hacer cambios a una aplicación sin documentarlos, porque no existe ningún procedimiento de control de cambios. Esta política asume que la palabra "crítica" se ha definido en la documentación de planificación de contingencias.

Políticas Relacionadas: “Aplicaciones de Producción Multiusuario” y “Programas de Aplicación de Usuarios Finales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Envío de Información Privada y Confidencial

Política: La información privada y confidencial debe ser enviada vía correo interno o externo en un sobre opaco y sellado, donde se indique claramente "Sólo para ser Abierto por el Destinatario".

Comentario: Esta política da instrucciones específicas a los trabajadores de la Empresa X sobre la manera apropiada para rotular la información privada y confidencial que se envía por varios tipos de correo, excepto el correo electrónico. Esta política se usa para la información sensible, pero no para el tipo de información más sensible. Una envoltura opaca evita que personas no autorizadas vean el contenido a través del sobre. El uso de la palabra "sellado" indica que no se deben emplear sobres re-usables que no serían apropiados para este tipo de aplicación. Es importante que el receptor sepa si una persona no autorizada ha examinado el material durante su recorrido. La política aquí mostrada presume la existencia de una política que defina los términos "privado y confidencial". Estos términos pueden ser fácilmente reemplazados con etiquetas comparables de uso común dentro de la organización.

Políticas Relacionadas: “Envío de Información Secreta” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Envío de Información Sensible Vía Fax — Notificación

Política: Si se envían documentos por fax con información secreta, se debe notificar al receptor el momento en que será transmitida. También se debe convenir que una persona autorizada estará presente en la máquina de destino cuando el material sea transmitido, a menos que la máquina fax esté restringida físicamente, de tal manera que aquellas personas que no estén autorizadas para ver el material transmitido no puedan entrar.

Comentario: Una situación donde habría una divulgación accidental de la información sucede cuando el material sensible ha sido enviado por fax pero aún no recogido por el receptor correspondiente. Esta política garantiza que ninguna persona no autorizada examinará los materiales sensibles transmitidos por fax. Si el receptor sabe que el fax está en camino, se preocupará si éste no llega a tiempo. La política asume la existencia de

otra política que defina el término "secreto". Este término puede ser fácilmente reemplazado con la etiqueta usada en la organización.

Políticas Relacionadas: "Envío de Información Sensible Vía Fax — Presencia Humana," "Envío de Información Sensible Vía Fax — Seguridad Física," "Envío de Información Sensible Vía Fax — No Cifrada," y "Registros de Faxes"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Envío de Información Sensible Vía Fax — Presencia Humana

Política: No debe transmitirse por fax información sensible, a menos que un miembro autorizado del grupo esté presente para que maneje apropiadamente los materiales o se use un buzón de fax protegido por una contraseña con el fin de restringir la entrega no autorizada del material.

Comentario: Una situación donde habría una divulgación inadvertida de información sucede cuando un material delicado se ha enviado por fax pero aún no ha sido recogido por el receptor indicado. Esta política exige la presencia de una persona o de un buzón protegido por una contraseña. En referencia a la primera opción, la política podría modificarse para exigir que el remitente confirme la presencia de un miembro autorizado del grupo, por teléfono y antes de la transmisión. Una opción más estricta sería prohibir la transmisión por fax de la información sensible, a menos que ambas máquinas de fax, la remitente y la receptora, empleen cifrado.

Políticas Relacionadas: "Envío de Información Sensible Vía Fax — Notificación"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

8. Envío de Información Sensible Vía Fax — Intermediarios

Política: No se debe transmitir por fax la información sensible de la Empresa X a través de intermediarios no confiables, lo cual incluye, sin limitantes, a personal hotelero y personal de las tiendas de alquiler de buzones de correo.

Comentario: Los trabajadores pueden estar en viaje de negocios, contar con poco tiempo y no darse cuenta de terceros que pudieran estar en contacto con la información sensible. La política podría extenderse para incluir otros métodos para el envío de información, por ejemplo, el uso de servicios de mensajería. El uso de cifrado es irrelevante en este caso porque los intermediarios pueden leer la información en forma impresa.

Políticas Relacionadas: "Envío de Información Sensible Vía Fax — Notificación" y "Envío de Información Sensible Vía Fax — Presencia Humana"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Envío de Información Sensible Vía Fax — Hoja de Cubierta

Política: Cuando deba transmitirse la información sensible por fax, dicha transmisión deberá estar precedida por una portada y confirmada por el receptor, después de lo cual el resto de la información sensible puede ser enviada mediante una segunda llamada.

Comentario: Esta política garantiza que la información sensible será enviada a la máquina de fax correcta. La política evita que llamadas no autorizadas interfieran con la vía de comunicación del fax. Con tantas máquinas de fax en uso hoy en día, es muy alta la posibilidad de equivocar el número y conectarse con otra máquina fax en una ubicación desconocida. Otro propósito de esta política es asegurarse que una persona autorizada vigile la máquina fax de destino. Esto evita que personas no autorizadas vean el contenido del material transmitido por fax. Es conveniente confirmar que se encuentra una persona autorizada en el sitio de recepción en caso que la segunda llamada no sea exitosa. Esta política podría ser complementada con otra frase que exija que el receptor acuse recibo de la segunda transmisión. La política no especifica cómo la persona acusará el recibo. Esta podría hacerse a través de una línea separada o por medio de un buscapersonas.

Políticas Relacionadas: "Envío de Información Sensible Vía Fax — No Cifrada" y "Envío de Información Sensible Vía Fax — Presencia Humana"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Envío de Información Sensible Vía Fax — No Cifrada

Política: La información sensible puede ser transmitida por fax a través de líneas no cifradas sólo cuando el tiempo apremie, cuando no se disponga de métodos de transmisión alternos y de mayor seguridad, y cuando se establezca un contacto de voz con la persona receptora inmediatamente antes de la transmisión.

Comentario: Esta política notifica al personal que no deben transmitir por fax información sensible por líneas no cifradas, de manera regular. Si existe una necesidad de transmitir de manera regular la información sensible, entonces los trabajadores deberían solicitar máquinas de fax criptografiadas. Algunas restricciones pueden aplicar a la exportación internacional de tecnologías de cifrado. La política aquí mostrada puede exigir también que se incluya el acuse de recibo del fax que contiene información sensible. Transmitir a una máquina fax autónoma, pudiera ser preferible a transmitir a un servidor de fax si éste no tiene controles de acceso adecuados y al cual puede llegar fácilmente un buen número de personas. Esta distinción puede ser establecida de manera explícita en esta política.

Políticas Relacionadas: “Envío de Información Sensible Vía Fax — Notificación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

11. Envío de Información Sensible Vía Fax — Seguridad Física

Política: La información secreta o confidencial no debe ser enviada a una máquina fax desatendida, a menos que la máquina de destino esté en un salón cerrado cuyas llaves sólo estén en posesión del personal autorizado para recibir la información.

Comentario: Esta política garantiza que sólo las personas autorizadas examinarán la información sensible. Al restringir físicamente el acceso, se impedirá a las personas no autorizadas ver los faxes confidenciales o secretos. Esta política no menciona nada sobre notificar al receptor. La política presume la existencia de una política que defina los términos "secreto" y "confidencial".

Políticas Relacionadas: “Envío de Información Sensible Vía Fax — Notificación,” “Clasificación de Datos en Cuatro Categorías,” e “Impresión de Información Sensible”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Envío de Información Secreta Vía Fax — Cifrado

Política: La información secreta no debe ser enviada por fax, a menos que la transmisión esté cifrada a través de los métodos aprobados por el departamento de Seguridad Informática de la Empresa X.

Comentario: El cifrado impide que la información sensible sea divulgada, al evitar que los espías y otros tengan acceso a ésta durante su transmisión por medio de servicios telefónicos. En el sitio de destino, la información se puede descifrar o se puede recuperar al invertir el proceso de cifrado. Aun cuando la transmisión esté cifrada, la información proveniente de la máquina de fax será legible por cualquier persona que esté presente cuando se reciba el fax. Para prevenir esto, se pueden exigir controles adicionales, como una contraseña, para poder imprimir el fax. Esta política frustra el espionaje de la línea de transmisión del fax. Es relativamente fácil colocar un sistema interruptor de línea para espiar la transmisión del fax y más tarde alimentar esta grabación a otra máquina de fax para generar una impresión legible. Si esto se hiciera, ni el remitente ni el receptor estarían al tanto que se ha interrumpido la línea. Este comentario es igualmente cierto en los nuevos servicios de transmisión por fax que usan Internet en lugar de líneas telefónicas convencionales. La política presume la existencia de una política que define el término "secreto".

Políticas Relacionadas: “Envío de Información Sensible Vía Fax — Seguridad Física,” “Clasificación de Datos en Cuatro Categorías,” “Información Secreta en Correo Electrónico,” y “Cifrado de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

13. Información Confidencial Vía Fax — Discado Rápido

Política: Cuando se envíe información confidencial vía fax, el operador no debe utilizar los números telefónicos de destino preestablecidos, sino que debe marcarlos manualmente.

Comentario: Ésta política evita enviar un fax a un número equivocado por un marcado erróneo. Este tipo de error pudiera dar como resultado una situación engorrosa donde, por ejemplo, un cliente importante se entera que a otro cliente importante le están ofreciendo un producto a un precio menor del que él pagó el día anterior. Otro caso lo constituye el envío equivocado de un contrato de fusión confidencial a un diario de negocios. Si los operadores de fax marcan manualmente el número de teléfono, ellos pueden fallar, pero este error es probable que se limite a un solo dígito, lo cual ocasionaría que el fax no pase porque se comunica con una línea de voz o de módem en lugar de otra línea de fax. No obstante, no existe este tipo de protección automática cuando se programan los números de fax.

Políticas Relacionadas: “Envío de Información Secreta Vía Fax — Cifrado” y “Registros de Faxes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

14. Envío de Información Secreta Vía Fax — Contraseñas

Política: La información secreta no debe ser enviada por fax a menos que, previo a su transmisión, la máquina receptora responda con una contraseña de manera exitosa.

Comentario: La política garantiza que se logrará la conexión con la máquina de fax correspondiente. Se han reportado casos donde faxes con información sensible han sido enviados a las máquinas equivocadas. Probablemente se requieran dos máquinas compatibles, cada una con soporte de contraseñas. Esto reducirá el número de máquinas a las que se puedan enviar faxes secretos y por ende también la posibilidad de error. Se requiere otra contraseña para la impresión de estos faxes. La política asume la existencia de una política que define el término "confidencial".

Políticas Relacionadas: “Envío de Información Sensible Vía Fax — Seguridad Física,” “Clasificación de Datos en Cuatro Categorías,” “Aviso en Cubierta de Fax,” y “Registros de Faxes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

15. Aviso en Cubierta de Fax

Política: Todos los faxes salientes de la Empresa X deben incluir una portada que incluya un párrafo informativo elaborado y aprobado por el departamento Legal.

Comentario: Esta política intenta responder efectivamente al importante número de faxes enviados a números equivocados. Esto no sólo implica marcar el número equivocado sino que puede también implicar fallas del sistema telefónico, sistemas de correo interno que envían faxes de manera incorrecta o el monitoreo que realizan los empleados de la compañía telefónica. Una portada normalizada garantizará que un texto legal precede todos los faxes salientes. Típicamente una portada de fax incluye un aviso que la transmisión sólo es para uso de una persona en particular o una entidad específica. Este aviso puede indicar también que si el lector del fax no es a quien está dirigido el mismo, entonces el lector no debe usar, diseminar, distribuir o copiar dicha información. El aviso puede exigir que se notifique al remitente si el fax ha sido enviado a otro sitio además del destino original. Se puede complementar el aviso con una frase que solicite destruir el fax enviado por error y que no se tome ninguna acción en base a la información contenida en dicho fax. La política antes mostrada brinda la mayor flexibilidad, puesto que se puede cambiar el párrafo de la portada sin tener que modificar la política como tal. Después de cierto tiempo, puede que cambie el contenido del párrafo de la portada, debido a la evolución del estatus legal del fax y del negocio.

Políticas Relacionadas: “Envío de Información Secreta Vía Fax — Contraseñas” y “Comunicaciones Potencialmente Ofensivas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

16. Información Secreta en Altavoces Telefónicos

Política: La información secreta no se debe discutir utilizando el altavoz de los teléfonos, a menos que las partes involucradas se aseguren de que personas no autorizadas no se encuentran en los alrededores de tal manera que puedan escuchar la conversación.

Comentario: Esta política evita divulgar información secreta no autorizada a través del altavoz de los teléfonos. Estos dispositivos a menudo se utilizan en oficinas abiertas, en las oficinas de recepción o en otras ubicaciones donde los transeúntes pueden escuchar la

conversación. El alcance de esta política pudiera extenderse y ser aplicada a teleconferencias y otras comunicaciones a través de altavoces de teléfonos. Se recomienda cifrar las líneas de teléfono en circunstancias durante las cuales se esté discutiendo información secreta. Para cumplir esta política, al comienzo de una conversación secreta, las partes involucradas deben asegurarse de la ausencia de personas no autorizadas en los alrededores. De la misma manera, si se inicia un conversación telefónica normal y a lo largo de la misma llega a ser necesario la discusión de información secreta, se debe realizar la afirmación anterior en ese mismo momento. La política asume la existencia de otra política que define el término "secreto".

Políticas Relacionadas:“[Clasificación de Datos en Cuatro Categorías](#)” e “[Información Sensible en Máquinas Contestadoras](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

17. Estaciones de Trabajo Sin Discos

Política: Todos los trabajadores del departamento de Investigación y Desarrollo deben utilizar estaciones de trabajo sin discos de almacenamiento, conectadas a una red departamental aislada, al trabajar en proyectos y tareas de desarrollo de productos nuevos.

Comentario: Esta política evita que los trabajadores abandonen la empresa llevándose consigo diseños nuevos de productos y otras informaciones altamente restringidas. Esto podría ser utilizado en otros entornos de alta seguridad tales como un departamento de Planificación Estratégica, un departamento de fusiones y adquisiciones o un departamento de estrategia de batalla militar. Al utilizar estas estaciones de trabajo sin discos de almacenamiento, los trabajadores no pueden almacenar información en un disco flexible u otro medio y llevársela. Como la red de trabajo es aislada, los trabajadores no pueden anexar esta información a un mensaje de correo electrónico para enviar una copia a un sitio fuera de la empresa. A través de la política, se logra un grado de privacidad que no se obtiene en muchas oficinas y como tal, provee un grado mayor de seguridad. Cuando estos trabajadores usen el correo electrónico o Internet, deberán utilizar otros computadores que no estén conectados a estas estaciones de trabajo. En aquellos casos donde se necesite postear o remover información del exterior en el servidor de la red de trabajo aislada, el administrador de sistema deberá realizar esta tarea.

Políticas Relacionadas:“[Operadores de Entrada de Datos](#)” y “[Equipos en Áreas de Información Secreta](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

18. Información Sensible al Tiempo

Política: La información de mayor confidencialidad que sea sensible al tiempo no se debe enviar por correo electrónico, correo de voz, teléfono u otros sistemas informáticos, hasta que no se hayan anunciado públicamente sus detalles.

Comentario: Esta política reconoce que la información está sujeta a cambios y como resultado de esto, a menudo no se puede confiar en la misma. La política indica a la gerencia que no debe utilizar sistemas informáticos para manejar tal información hasta que la misma sea publicada. A pesar de que los programas de cifrado y otros controles automáticos tienen el potencial de proteger la información de manera más segura, esos controles pueden ser usados incorrectamente, resultando en la publicación accidental de dicha información. Esta política puede ser utilizada de una mejor manera, si se adopta de acuerdo con cada proyecto, más que como política normal tomada directamente del manual. La política no debería aplicarse a menos que las palabras "mayor confidencialidad" hayan sido definidas de antemano. Otras palabras tales como "máximo secreto" pudieran ser usadas en su lugar. Otro beneficio de esta política es que no quedan rastros electrónicos de eventos u otras informaciones que pudieran ser descubiertos a lo largo de un proceso legal.

Políticas Relacionadas:“[Destrucción de Información](#)” y “[Sistemas Secretos](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

19. Almacenamiento de Información Sensible

Política: Los trabajadores de la Empresa X no deben almacenar información privada, confidencial o secreta en la unidad de disco duro de un computador personal o estación de trabajo, a menos que la Gerencia de Seguridad Informática haya determinado que se han utilizado las medidas de seguridad informática adecuadas.

Comentario: Debido a que los computadores personales (PC) y las estaciones de trabajo no proporcionan el mismo nivel de seguridad que los servidores o los

sistemas centrales de uso departamental, algunas organizaciones prohíben almacenar información en los mismos, a menos que se apliquen los controles adecuados. Esta política exige el uso de los controles adecuados, tales como el uso de programas de control de acceso basados en contraseñas. La intención no es prohibir el almacenamiento de información confidencial en unidades de disco duro, sino prestarle una atención especial a estas unidades ya que las mismas no pueden ser fácilmente bloqueadas al final del día laboral. Se debe prestar atención especial cuando un PC o estación de trabajo estén conectados a una red de área local, en cuyo caso otros usuarios pueden examinar el contenido de una unidad de disco duro ajena. La política es deliberadamente vaga en cuanto a cuáles medidas de control específico resultan más adecuadas, porque se espera que éstas cambien con el tiempo.

Políticas Relacionadas: “Cifrado de Almacenamiento en Disco”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

20. Grabación de Información Sensible

Política: Los trabajadores no deben grabar información sensible en ningún tipo de dispositivo de grabación, a menos que se especifique la clasificación de sensibilidad apropiada tanto al comienzo como al final de cada segmento de información sensible, el medio de grabación se identifique con la más estricta clasificación de datos grabados en el medio, el medio se proteja de conformidad con la más estricta clasificación de datos grabados en el medio y el medio se borre tan pronto como sea posible.

Comentario: Esta política previene el uso de dispositivos de grabación para información sensible. Si no se puede eludir el uso de estos sistemas, entonces se deben tomar las precauciones estipuladas en la política, las cuales no serán necesarias si los medios han sido cifrados o aleatorizados. Los rollos de cinta, cintas de casete y otros medios de grabación pueden ser fácilmente robados o copiados, comprometiendo la información sensible a ser publicada sin autorización. Para un nivel mayor de seguridad, el requisito en la política de borrar el medio tan pronto como sea posible, se puede reemplazar con frases que instruyan al usuario a destruir el medio de acuerdo con métodos autorizados.

Políticas Relacionadas: “Información Sensible en Máquinas Contestadoras”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

21. Consumo Excesivo de Recursos

Política: Las actividades de los usuarios no privilegiados en los sistemas de computación compartidos, no deben causar retardos o interrupciones en el suministro de servicios a otros usuarios.

Comentario: Aunque esta política se refiere a la ubicación apropiada de los controles de acceso, también se refiere a las acciones que los usuarios finales están capacitados para iniciar. Por ejemplo, un usuario único de un sistema central no debería consumir todos los recursos del sistema de tal manera que otros usuarios no puedan obtener servicio de procesamiento. Esta política dirige las maneras en que se establecen los controles de acceso, la manera en que se asignan los recursos del sistema y las maneras de diseñar los sistemas de aplicaciones. Los gusanos, los virus y otros programas no autorizados, a menudo consumen demasiados recursos del sistema, llevando a la suspensión del servicio a los usuarios. Si el sistema ha sido configurado para prevenir este tipo de suspensión de servicios, entonces el administrador del sistema estará en conocimiento de que existen problemas.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer” y “Consumo de Recursos por Programas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

22. Respaldo de Computadores Portátiles

Política: Los trabajadores que usen computadores portátiles deben preparar copias de respaldo de toda la información crítica antes de emprender viajes de negocios, almacenando dichas copias en algún sitio diferente al maletín del computador portátil.

Comentario: Esta política garantiza que la información crítica almacenada en el disco duro de una máquina portátil no se perderá cuando un computador portátil se extravíe o sea robado. Esto sucedería si el evento ocurrió mucho tiempo después de la última copia de respaldo del disco duro. Esta política también protege en el caso de que un computador portátil sea confiscado por agentes de la policía o de aduana, en cuyo caso la información así almacenada no estaría disponible para transacciones comerciales. Esta política utiliza los viajes fuera del sitio de trabajo como un motivo para elaborar una copia adicional de respaldo. Este motivo pudiera no

ser conveniente para el personal de ventas u otros trabajadores que viajan prácticamente todos los días. Para esta gente, el motivo más bien pudiera ser un viaje fuera del estado o fuera del país.

Políticas Relacionadas: “[Computadores Portátiles en Aviones](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

23. Copias de Información Sensible, Crítica o Valiosa

Política: A menos que se tenga conocimiento de que estén operativas otras formas de respaldo, todos los usuarios finales son responsables de realizar por lo menos dos copias de respaldo actualizadas de archivos críticos cada vez que se lleve a cabo un número significativo de cambios.

Comentario: Esta política permite que los usuarios finales se encarguen de gran parte del trabajo de reconstrucción de datos ya que poseen dos o más copias de respaldo de información sensible, crítica o de archivos valiosos. La política también constituye una mayor seguridad de respaldo para las modificaciones de los archivos importantes que aún no han sido respaldados a un servidor o a un sistema de respaldo con unidad de cinta ubicado en el propio computador personal (PC) o estación de trabajo. Para que sea efectiva, esta política necesitará también de cierto adiestramiento por parte de los usuarios en cuanto a respaldos. Los requisitos específicos de esta política no presentan mayor dificultad. Por ejemplo, los usuarios de un PC o estación de trabajo pueden almacenar una copia en su unidad de disco duro y otra en un servidor de red local, o pueden almacenar una copia en un disco flexible y una copia en su unidad de disco duro. En realidad resulta económico para muchos usuarios finales el uso de dos o más unidades de disco duro. Esta política es importante para aquellos casos en los que una copia de respaldo automático se realiza a nivel de una red local o de una red extensa, sin involucrar al usuario. Esta política asume que la palabra "crítica" ha sido definida en otro sitio.

Políticas Relacionadas: “[Archivos Críticos de Respaldo](#),” “[Clasificación de Datos en Cuatro Categorías](#),” y “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

24. Revisión del Respaldo

Política: Los gerentes de Departamento o sus delegados deben responder por la elaboración de los respaldos adecuados de datos sensibles, críticos y valiosos, si tal información está almacenada en computadores personales, estaciones de trabajo u otros sistemas pequeños.

Comentario: A menos que se recuerde o se exija a los usuarios finales hacer respaldos con regularidad, puede que no lo hagan. A menudo, los usuarios finales no entienden la necesidad de realizar los respaldos de archivos hasta que sufren una pérdida importante de información. Esta política evita estas pérdidas mayores de información y las consecuencias resultantes. La política se puede complementar con un adiestramiento adecuado del usuario en cuanto a respaldos. Algunos sistemas pueden respaldar automáticamente los cambios hechos por los usuarios, almacenando las copias más recientes en un servidor al final del día de trabajo. De usarse este mecanismo automático, esta política exige que la gerencia garantice la efectividad de este proceso. La política asume que la palabra "crítico" se ha definido en otro sitio.

Políticas Relacionadas: “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#),” “[Respaldos Automáticos](#),” y “[Respaldo de Datos](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

25. Confirmación de Cambio de Dirección

Política: Las solicitudes de cambio de dirección de correspondencia por parte de los clientes se deben hacer efectivas un mes después de ingresar el cambio al sistema, y las solicitudes de cambio de dirección de correo electrónico se harán efectivas dos días hábiles después de ingresar el cambio al sistema, confirmándose ambas acciones mediante un aviso enviado a la dirección anterior.

Comentario: Esta política garantiza que personas no autorizadas no tengan éxito al solicitar cambios de dirección. Las solicitudes de cambio de dirección ficticias a menudo son esenciales para cometer un fraude, tal como es el caso de una solicitud fraudulenta de una tarjeta de crédito. Esta política le permite a la persona autorizada en la toma de decisiones sobre la cuenta, la oportunidad de corregir cualquier error o irregularidad antes de que el cambio sea efectivo. Una confirmación del cambio de dirección debe enviarse de inmediato; sin embargo, un retraso en un cambio de

dirección de correo normal no representaría un problema ya que se puede disponer de reenvío de correo. Puede suceder que algunas de estas comunicaciones sean devueltas como resultado de esta política, pero esto se puede resolver con prontitud ya que la nueva dirección estará incluida en la base de datos de clientes de la Empresa X.

Políticas Relacionadas: “Canal de Confirmación” y “Validación de la Identidad de Terceros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

26. Numeración de Líneas en Mensajes Críticos

Política: Se debe numerar cada línea de los mensajes de texto con formato libre, relativos a asuntos críticos o particularmente importantes del negocio.

Comentario: La numeración de líneas de textos de formato libre o sin formato, se han utilizado por largo tiempo en los documentos legales para garantizar que todos los cambios sean claramente evidentes. Algunos sistemas usan este mecanismo como parte del propio mensaje. Si la generación de números de línea no es automática, los usuarios pueden agregarle números a la izquierda de cada línea usando procesadores de palabras, editores de texto y programas similares. Algunas redes multiorganizacionales importantes, tales como los sistemas de intercambio de información electrónica, pudieran incluir numeración de línea para todos los mensajes de texto en formato libre. Algunos documentos legales también emplean la numeración para resaltar cambios y hacer más fácil las referencias cruzadas.

Políticas Relacionadas: “Entrada con Doble Tecla de Transacciones Mayores,” “Investigación de Errores,” y “Errores y Manipulación de Registros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

27. Derecho a la Libre Expresión

Política: Los sistemas de computación y de comunicaciones de la Empresa X no se deben usar en el ejercicio del derecho de la libre expresión de los usuarios.

Comentario: Esta política notifica a los usuarios del sistema que la gerencia no respaldará el ejercicio de sus derechos de expresarse libremente al usar los sistemas

de la Empresa X. En su lugar, esta política permite a la Empresa X editar o censurar los correos electrónicos, las publicaciones en los foros electrónicos, los sitios de la intranet y los correos de voz. Esta política elimina dudas acerca de los problemas legales asociados a la violación de la libertad de expresión. Otra situación donde se aplicaría esta política es en el envío de mensajes inapropiados o censurables vía Internet. La política disuade a los usuarios de hablar libremente al usar los sistemas de la Empresa X, lo que puede ser una política sensata si la Empresa X desea eludir asuntos judiciales.

Políticas Relacionadas: “Censura de Datos” e “Información Sobre Libertad de Expresión”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

28. Censura de Datos

Política: La gerencia de la Empresa X no debe permitir el uso de computadores o redes de trabajo como foros públicos de sus usuarios finales y se reserva el derecho a censurar cualquier información ingresada en ellos.

Comentario: La intención de esta política es que los sistemas organizacionales no se conviertan en mecanismos que puedan dañar a la empresa. Esto podría suceder si se conectan simultáneamente miembros de un sindicato, un grupo de clientes descontentos, una fracción minoritaria de accionistas o algún otro grupo de particulares descontentos con la gerencia actual. Otra intención es poder impedir ciertos usos del sistema de ser éstos contrarios a la política de la Empresa X o a la ley. Por ejemplo, si un sistema se usa para intercambiar números robados de tarjetas de crédito, la gerencia querrá censurar los mensajes producto de esta actividad.

Políticas Relacionadas: “Derecho a la Libre Expresión,” “Avisos Públicos Inadecuados,” y “Sin Responsabilidad en Mensajes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

29. Remoción de Material Ofensivo

Política: La Empresa X deberá conservar el derecho de eliminar de sus sistemas de computación cualquier material percibido como ofensivo o potencialmente ilegal.

Comentario: Esta política está orientada a notificar a los usuarios que la gerencia no tiene la obligación de conservar información almacenada en sus sistemas si considera que dicha información es ofensiva, ilegal o cuestionable. Esta política no indica que el operador del sistema ejercerá un control editorial, que el operador revisará material para determinar en qué caso satisface normas de la comunidad o en qué caso el operador aplicará alguna norma particular de decencia. La política simplemente brinda a la organización el derecho de eliminar material a discreción. En la mayoría de los casos esto será una respuesta a una queja o una advertencia suministrada por otro usuario. La política deliberadamente no dice nada sobre darle al usuario comprometido un aviso por adelantado o en el momento del proceso de remoción. Esta política es particularmente importante en aquellas organizaciones que operan foros electrónicos, salones de charla en línea, páginas en Internet con áreas de interacción con los usuarios y otros sistemas que ponen esta información a la disposición de un amplio público.

Políticas Relacionadas: “Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización,” “Información y Software No Autorizados,” y “Comunicaciones Potencialmente Ofensivas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

30. Responsabilidad de Monitorear Contenido

Política: La Empresa X nunca debe estar obligada a monitorear el contenido de la información que resida o fluya por sus sistemas informáticos, pero debe conservar el derecho de eliminar cualquier mensaje, archivo, base de datos, gráfico o algún otro material de sus sistemas informáticos.

Comentario: La finalidad de esta política es darle a la gerencia el máximo de flexibilidad para eliminar con prontitud material de sus sistemas informáticos. Al mismo tiempo, la declaración de este derecho de eliminar material no debe hacerle creer al lector que todos los contenidos serán monitoreados. Esta política reconoce que las normas comunitarias, un término legal asociado a la censura y las normas de negocio, evolucionarán con el tiempo. Esta política no necesita cambiar aunque las normas mencionadas lo hagan. La posición legal que esta política trata de establecer, es la de una operadora común, tal como una de compañía telefónica. La compañía telefónica no es responsable por el uso

ilegal o no ético de sus equipos. De esta manera, esta política es aplicable a un proveedor de servicios de Internet, una red con valor agregado, un operador de foro electrónico o una organización similar.

Políticas Relacionadas: “Normas de Telefónicas Comunes” y “Avisos Públicos Inadecuados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

31. Sincronización de Dispositivos

Política: Los sistemas que automáticamente intercambian información entre dispositivos, tal como un asistente personal digital y un computador personal, no deben habilitarse a menos que los sistemas hayan sido evaluados y autorizados por el departamento de Seguridad Informática.

Comentario: Esta política evita la divulgación accidental de información sensible a terceros no autorizados y previene problemas operacionales que pudieran evitarse. La política surge del reciente desarrollo de una gran variedad de equipos que automáticamente sincronizan archivos entre varios dispositivos, incluyendo computadores de mano. Aunque estos sistemas emplean tecnologías útiles y atractivas, pueden accidentalmente divulgar información a personas no autorizadas. Por ejemplo, si una transmisión de radio se inicia autónomamente entre dos dispositivos y si esta transmisión no se codifica, la información enviada puede ser interceptada y usada por un tercero. Igualmente, a menos que los dispositivos empleen un mecanismo de identificación, la información puede ser transferida a los dispositivos equivocados, sobre escribiendo archivos, destruyendo información importante y potencialmente causando problemas operacionales. Una evaluación por parte del departamento de Seguridad Informática asegura que estos sistemas incorporan los controles necesarios para estar en concordancia con las medidas de seguridad informática existentes en la organización. Esta política no prohíbe el uso de dispositivos que tengan estas características, sino que simplemente solicita de los usuarios no utilizar esta capacidad sin permiso previo.

Políticas Relacionadas: “Sincronización del Reloj” y “Transmisión Inalámbrica de Información Secreta”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

32. Llamadas Cobro a Destino y a Terceros

Política: Los administradores a cargo de los sistemas de correo de voz de la Empresa X deben hacer arreglos con la compañía telefónica involucrada en ambos tipos de llamadas - por cobrar y con cobro a terceros - para que éstas no se puedan realizar en las líneas telefónicas de correo de voz.

Comentario: Cuando los hackers irrumpen en un sistema de correo de voz, a menudo crean sus propios buzones y graban mensajes salientes para aceptar llamadas por cobrar y por cobrar a terceros. Además de exigir contraseñas largas para todas las cuentas de usuario habituales y la cuenta del administrador del sistema, este último debe comunicarse con la compañía telefónica y solicitar la prohibición de las llamadas indicadas en esta política. Muchas compañías telefónicas lo harán sin recargo adicional. Algunas lo harán sólo si ha ocurrido algún abuso en el pasado. No hay necesidades de negocio que ameriten realizar este tipo de llamadas dentro de un sistema de correo de voz, así que la limitación impuesta por esta política sólo cierra una vulnerabilidad de seguridad que puede ser abusada. En algunos casos esta prohibición se puede aplicar a números de teléfono normales.

Políticas Relacionadas: “[Información Sensible en Máquinas Contestadoras](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

33. Llamadas a Servicios de Información

Política: Los administradores a cargo de centrales privadas de la Empresa X deben programar los sistemas PBX de tal manera que no se complete ninguna llamada a números de servicios informáticos.

Comentario: Esta política evita que se carguen a la Empresa X los servicios de llamadas de información no autorizados. En el proceso de prohibir esas llamadas, la Empresa X podría, sin intención, hacerle difícil a los empleados obtener cierta información que legítimamente necesiten para completar su trabajo. No obstante, esto es algo poco común y esas llamadas se pueden hacer mediante otros teléfonos, tales como teléfonos públicos con una tarjeta de crédito telefónica de la Empresa X. Esta política podría ser ampliada para incluir la prohibición de llamadas internacionales generadas desde ciertos teléfonos. Los teléfonos celulares cargados a la Empresa X pudieran tener bloqueada la capacidad de realizar llamadas internacionales.

Políticas Relacionadas: “[Llamadas con Tarjeta de Crédito](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

34. Areas Telefónicas

Política: Los números asequibles a través de las líneas privadas de la Empresa X deben restringirse sólo a aquellos necesarios para los objetivos normales del negocio.

Comentario: Esta política evita cargos telefónicos fraudulentos. Un buen número de fraudes identificados implican llamadas a los países menos industrializados desde negocios localizados en los países más industrializados. Siempre y cuando las actividades del negocio no sean afectadas indebidamente, las organizaciones pueden evitar fraudes bloqueando las llamadas a estos países menos industrializados. En algunas instancias, tales como en el caso de teléfonos celulares, es apropiado bloquear todo género de llamadas internacionales. En otras instancias, tal como un teléfono de acceso general ubicado en la propia fábrica, todas las llamadas nacionales de larga distancia pueden ser bloqueadas. En ciertas situaciones del negocio, tales como en almacenes minoristas, sólo se permitirán llamadas salientes y entrantes de emergencia. Los usuarios de teléfono pueden hacer uso de operadores si necesitan llamar a un área que ha sido bloqueada. Ciertos códigos de área que imponen cargos adicionales también pueden ser bloqueados selectivamente.

Políticas Relacionadas: “[Devolución de Llamadas de Larga Distancia](#)” y “[Restricción de Privilegios — Necesidad de Conocer](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

35. Almacenamiento de Mensajes de Correo Voz

Política: Los usuarios deben revisar su correo de voz por lo menos una vez al día ya que todos los mensajes de correo de voz serán borrados al cumplir éstos un mes.

Comentario: Esta política motiva a los usuarios de correo de voz a eliminar inmediatamente sus mensajes en el sistema, lo que evita el uso del sistema como base de datos. Este mecanismo agilizará las respuestas a las solicitudes de clientes, posibles clientes, vendedores y otros. Este mecanismo también minimizará la

información sensible almacenada en el sistema de correo de voz en un momento dado, lo que reducirá las posibilidades de divulgaciones no autorizadas. Esta política también disminuirá la necesidad de espacio en disco para un sistema de correo de voz, el cual a menudo opera en un computador personal.

Políticas Relacionadas: “[Remoción de Registros de Computadores Accesibles desde Internet](#),” “[Retención de la Información Personal](#),” y “[Destrucción de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

36. Llamadas con Tarjeta de Crédito

Política: Los trabajadores no deben realizar llamadas de discado directo con cargo a las tarjetas de crédito con un operador telefónico privado externo (PBX), sino a través de un teléfono público u otra línea directa.

Comentario: Esta política evita que los números de tarjetas de crédito telefónicas y los números de identificación personal (PIN, por sus siglas en inglés) queden grabados en registros de llamada. Esto impedirá que estos registros sirvan como fuente de números de tarjeta de crédito que puedan facilitar llamadas fraudulentas. Cuando se utilice un operador telefónico privado (PBX), los trabajadores pueden dar de palabra su número y PIN de tarjeta de crédito a un operador de la compañía telefónica, aunque se corre el riesgo de que alguien escuche los números. Por esta razón, el manejo de números en palabras no se aprueba en esta política. Esta no es una política popular porque resulta incómoda para los usuarios telefónicos, pero ayuda a minimizar los fraudes. En lugar de aplicar esta política, es suficiente para muchas organizaciones llevar un control detallado y periódico de la facturación de las tarjetas de crédito. El término "PBX" puede necesitar una definición más específica dependiendo a quien vaya dirigida esta política.

Políticas Relacionadas: “[Llamadas a Servicios de Información](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

37. Implantación del Acceso al Sistema Telefónico Directo

Política: En las sedes de la Empresa X no debe habilitarse la opción de acceso directo interno en las centrales telefónicas, a menos que estén acompañadas de un sistema de detección y limitación de fraudes, previamente autorizado por el gerente del departamento de Telecomunicaciones.

Comentario: Esta política evita el uso de servicios DISA, a menos que vayan acompañados de sistemas de detección de fraude y de inhabilitación de privilegios de usuarios. Muchos expertos en telecomunicaciones indican a los administradores de sistemas telefónicos que simplemente inhabiliten la opción DISA. Sin embargo, DISA puede en efecto ahorrarle a una organización una cantidad importante de dinero si se pone en práctica de manera segura. Esta política se basa en la suposición de que los usuarios responderán en el corto plazo de las pérdidas ocasionadas por un fraude. La necesidad de esta política se alteraría de ser aprobadas leyes que desplacen la responsabilidad del uso fraudulento del teléfono a los operadores de los sistemas telefónicos y fabricantes de centrales privadas (PBX), porque estos operadores y fabricantes probablemente reaccionarían incluyendo sistemas de seguridad adecuados dentro de sus equipos, en lugar de ofrecerlos como una opción. Adicionalmente, la necesidad de una política como ésta disminuiría con una cobertura de seguro contra el fraude telefónico, tal como la que recientemente ha sido provista por algunos operadores.

Políticas Relacionadas: “[Uso de Tarjetas de Crédito](#)” e “[Investigación de Delito Computarizado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

38. Ordenes para Cambiar Registros

Política: No deben ser procesadas las órdenes de cambio realizadas por teléfono sobre cualquier registro interno de la Empresa X, a menos que la identidad del interlocutor haya sido verificada mediante procedimientos autorizados.

Comentario: Esta política está orientada a definir las circunstancias bajo las cuales las transacciones telefónicas serán consideradas válidas y se usen como vía para actualizar registros internos. El proceso por el cual se verifica la identidad del interlocutor puede ser tan simple como suministrar su número de seguridad social o un número de teléfono, aunque ninguno de estos es totalmente efectivo porque esta información está

disponible públicamente. Es mejor la devolución de la llamada al tercero a un número predeterminado y entonces confirmar verbalmente que se puede proceder con la transacción. Pero aun esta opción puede ser frustrada mediante el desvío de la llamada. Para mayor seguridad, se recomienda emplear un código de contraseña predeterminada o de uso especial. Este proceso se emplea generalmente para colocar órdenes de transferencia de fondos bancarios por teléfono. El alcance de esta política se puede expandir para incluir órdenes vía fax y órdenes de correo electrónico. La confirmación de la identidad del interlocutor también se puede aplicar a aquellas circunstancias donde los interlocutores solicitan información sensible y de estricto uso interno.

Políticas Relacionadas: “Capacidad de Reconstrucción de Cambios en Producción” y “Cambios en Producción”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

39. Activación del Puente de Conferencias

Política: Los puentes de conferencia sólo deben ser activados cuando se necesiten y deben dejarse inactivos cuando no se les requiera.

Comentario: Esta política evita fraudes a través de llamadas no autorizadas. Un ardid popular actualmente en uso implica el abuso de un puente de conferencia que no ha sido inhabilitado al final de su uso. Este puente es entonces aprovechado por hackers que aceptarán llamadas por cobrar de terceros para otros hackers, quienes a su vez pueden colocar llamadas salientes no autorizadas mediante el puente y éstas serán eventualmente cargadas a la organización. Un puente de conferencia se puede usar también para disimular el trabajo de un hacker porque incrementa la cantidad de sistemas y redes diferentes penetradas por él. Ellos también pueden tomar control de un puente y hacer uso de éste para sus propios propósitos, tal como es el intercambio de números robados de tarjetas de crédito. Para frustrar esta actividad, los puentes de conferencia se pueden controlar con contraseñas u otros mecanismos de seguridad.

Políticas Relacionadas: “Acceso Remoto de Terceros” y “Sesiones Activas Desatendidas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

40. Cuentas Personales en un Proveedor de Servicios de Internet

Política: Aquellos trabajadores que deseen expresarse en un foro público en Internet acerca de cualquier tema que no involucre asuntos de negocio o intereses de negocio de la Empresa X, deben usar sus propias cuentas personales, suministradas por su proveedor de servicios de Internet y sus propias cuentas de correo electrónico para presentar tales declaraciones.

Comentario: Esta política evita que la gente que lea las declaraciones redactadas por los trabajadores de la Empresa X en un foro público de Internet, crea que tales declaraciones representan la opinión de la Empresa X o que son declaraciones oficiales emitidas por la Empresa X. El uso de una cuenta de correo electrónico de la Empresa X para hacer declaraciones personales implica que la organización respalda lo que un particular dice, aunque dicho apoyo oficial no exista. Esta política también reduce la probabilidad de alegatos de difamación y denigración en reclamos judiciales contra la organización. La política también respalda el derecho a la libertad de expresión, pero aclarando que tales declaraciones de libre expresión deben mantenerse distantes de la posición de la Empresa X. Esta política se debe acompañar por otra política que aclare que todos los usos del nombre de la Empresa X necesitan estar previamente autorizados.

Políticas Relacionadas: “Uso del Nombre de la Organización” y “Liberación de Información de la Organización”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

41. Transmisiones a Través de Correo Electrónico y Correo de Voz

Política: Los servicios de transmisión disponibles en los sistemas de correo electrónico y sistemas de correo de voz sólo deben ser usados por la alta gerencia o mediante su autorización.

Comentario: La finalidad de esta política es reducir el correo basura. La productividad de muchos trabajadores se ve impactada desfavorablemente por anuncios de baja prioridad. Para algunas organizaciones, esta política puede también restringir severamente el uso de medios de transmisión. Algunas organizaciones pueden redactarla de tal manera que permita el uso de las instalaciones en el evento de una emergencia o siniestro. Las organizaciones pueden optar por establecer un procedimiento formal de revisión y autorización para la

emisión de mensajes. Adicionalmente pueden otorgar tanto a los administradores del sistema como a los miembros del departamento de seguridad un permiso general para realizar estas emisiones sin la previa autorización de la alta gerencia. En algunos casos, las organizaciones pueden restringir los privilegios informáticos de los usuarios finales, permitiéndoles realizar estas emisiones. El alcance de esta política puede extenderse para regir los sistemas públicos, tales como los altavoces en los edificios.

Políticas Relacionadas: “Derecho a la Libre Expresión” y “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

42. Correo de Voz para Grupos

Política: Los mensajes de correo de voz o correo electrónico a enviar a grupos con más de 10 receptores, deben ser autorizados por un gerente de departamento.

Comentario: Esta política evita que los trabajadores envíen material erróneo, molesto o inapropiado a un gran número de receptores mediante sistemas de correo de voz o de correo electrónico. Con esta política, los gerentes de departamento están en la posición de interpretar y aplicar políticas de correo de voz y correo electrónico para aquellos trabajadores que no las puedan entender. Igualmente, esta política impone una cierta formalidad a esas comunicaciones que obligan a los trabajadores a pensar mejor antes de preparar un mensaje y buscar la autorización del gerente de departamento. Si el mensaje no es importante, entonces los trabajadores probablemente no se molestarán en obtener la autorización de la gerencia y los receptores potenciales no tendrán que preocuparse por otro artículo de material sin importancia. Esta política indirectamente evita el uso de los medios de transmisión, pero la política es más amplia en su alcance e incluye otros medios, tales como las listas de correo electrónico privado. La política se aplica a receptores de mensajes tanto internos como externos.

Políticas Relacionadas: “Foros Electrónicos Públicos” y “Aprobación de las Representaciones Públicas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

43. Ejecución de Código Móvil

Política: Los trabajadores no deben ingresar en procesos de Internet que involucren el uso de código móvil, permitir que el código móvil se ejecute en sus máquinas o permitir la colocación de código móvil en sus máquinas.

Comentario: Esta política está dirigida a dos tipos de código móvil: uno donde el usuario solicita el código y otro donde el usuario o software dirigido por el usuario, envía una solicitud de búsqueda a la red en busca de una respuesta. En ambos casos, el usuario en algún momento u otro solicita la ejecución del código móvil o por lo menos permite la operación de este tipo de código. En muchos casos, el usuario puede que no sepa que se trata de un código móvil y puede ser incapaz de elegir. El código móvil puede llegar a la máquina de un usuario por una variedad de rutas. Por ejemplo, el código móvil puede venir mediante una sesión de protocolo de transferencia de archivo o como un anexo de correo. Esta política prohíbe todo tipo de código móvil. Esta posición conservadora se justifica porque el código móvil puede ser hostil, al contener virus o gusanos. Además, muchas organizaciones no están preparadas para lidiar con las complejidades del código móvil. Esta política puede impedir ciertos tipos de diálogos comerciales en Internet. Se recomienda el filtrado para identificar el código móvil tanto en el cortafuegos como en el servidor de correos y debe usarse en adición a ésta política, que sólo está orientada al usuario final.

Políticas Relacionadas: “Ejecución de Programa Java” y “Contenido Activo en Sitios Intranet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

44. Publicaciones en Intranet

Política: Antes de publicar cualquier información en la intranet de la Empresa X, tanto el gerente encargado del departamento de la página pertinente en intranet como el Propietario de la información en cuestión deben aprobar su contenido.

Comentario: Esta política evita que los empleados publiquen información que no debe estar disponible en la intranet. Los procesos de autorización descritos en esta política le dan una oportunidad a la gerencia para revisar si la información pertenece a la página propuesta en intranet, si la información debería colocarse en la intranet y si se requiere algún control adicional para su acceso. Además de evitar la divulgación inapropiada de

información sensible, esta política mantendrá la colocación en intranet de información de manera organizada y consistente con los propósitos de negocios. Se recomienda un conjunto separado de lineamientos para seleccionar la información a ser colocada en la intranet. Este conjunto de lineamientos se puede distribuir a los gerentes de departamento con páginas web en la intranet para que así puedan llevar a cabo de manera más apropiada sus deberes, de acuerdo a lo señalado en esta política.

Políticas Relacionadas: “Avisos Públicos Inadecuados” y “Publicación en Internet de Material”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

45. Propiedad del Contenido de Intranet

Política: Todo el contenido colocado en la intranet de la Empresa X es propiedad de la Empresa X, a menos que otra cosa haya sido previamente autorizada por el director del departamento de Servicios informáticos y explícitamente indicado en la página web de la intranet.

Comentario: La política elimina controversias acerca de quién es el Propietario del contenido colocado en las páginas web de la intranet. Es aconsejable para una organización el mantener la propiedad del contenido para así poder censurarlo cuando sea necesario. Aunque no se prevea disputa acerca de asuntos de violación de derechos de autor o difamación, puede haber disputa sobre la calidad del contenido por ser de mal gusto, pobre criterio o por ofrecer una imagen negativa de la Empresa X. Si la Empresa X posee páginas web en su intranet, también puede ser responsable por su contenido. Esto implica que debe haber un proceso de revisión previo al envío de material a la intranet.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

46. Validación de Información en Intranet

Política: Antes de enviar material a la intranet, los trabajadores deben asegurarse de que la información y los programas no contengan código malicioso, confirmar su exactitud, oportunidad y pertinencia para el negocio de la Empresa X y resolver todos los asuntos legales relacionados con dicha información.

Comentario: Esta política define los pasos de control de calidad que los usuarios deben tomar antes de colocar cualquier cosa en la intranet. La política asume que los usuarios pueden colocar algo en la intranet sin pasar por un comité de revisión o algún otro proceso de autorización. A pesar de que no se recomienda que todos los usuarios obtengan permiso para colocar lo que quieran en intranet, esta política puede ser usada por organizaciones que empleen este enfoque. Se pueden suministrar herramientas normales para su empleo en la verificación de código malicioso y tal vez mencionarlo en la política. La política asume que la información personal se mantiene fuera de la intranet. De no ser así, las palabras “pertinencia para el negocio de la Empresa X” pueden ser borradas.

Políticas Relacionadas: “Propiedad Intelectual” y “Publicaciones en Intranet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

47. Revisión y Prueba de Contenido de Intranet

Política: Todo el contenido nuevo o cambiado a enviarse a la intranet de la Empresa X debe pasar por un área de prueba, donde personal autorizado revisará el contenido y pondrá a prueba su operación, a menos que se haya obtenido autorización escrita de la gerencia de Seguridad Informática.

Comentario: Esta política notifica a los trabajadores que la intranet es un sistema de producción que requiere procedimientos formales de control de cambios. Esta política restringe el contenido de intranet, así que sólo se puede colocar material de alta calidad. La política permite que sólo se coloque contenido que haya sido filtrado y cuya precisión, importancia, vigencia y la no violación de las políticas de seguridad interna hayan sido demostradas. Aunque no esté establecido en la política, el acceso al área de prueba debe restringirse con mecanismos tales como acceso a directorios de archivo controlados por contraseñas. Las palabras en la política “donde personal autorizado revisará el contenido” implica eso, pero no lo exige.

Políticas Relacionadas: “Cambios en Producción” y “Entregas al Centro de Computación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

48. Contenido de Internet Trasladado a Intranet

Política: Todo el contenido que se descargue desde Internet debe pasar por un proceso de depuración estructurado y documentado, antes de su colocación en la intranet de la Empresa X.

Comentario: Esta política garantiza que el contenido descargado desde Internet no contendrá virus, gusanos y otros objetos maliciosos que puedan propagarse a través de los sistemas de escritorio en la Empresa X. Aunque el proceso de depuración debe incluir el uso de paquetes de detección de virus, debe implicar también la extracción de contenido dinámico o por lo menos su detección. Esos subprogramas de contenido dinámico pueden ocultar código malicioso que ocasionaría daños a los sistemas de la Empresa X. El proceso de depuración debe incluir, además, un examen visual del contenido descargado para que pueda ser recolocado internamente sin restricción.

Políticas Relacionadas: “[Sistema de Prueba Antivirus](#)” e “[Información Usada en Pruebas de Software](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

49. Contenido Activo en Sitios Intranet

Política: Sólo aquellos subprogramas de contenido activo que hayan sido probados y autorizados por el departamento de Sistemas Informáticos pueden ser usados en los sitios conectados a la intranet de la Empresa X.

Comentario: Esta política garantiza que los programadores que trabajen para un departamento o alguna otra unidad organizacional descentralizada, no incorporarán subprogramas de contenido activo en un sitio de intranet que, al ejecutarse, propaguen virus, gusanos o algún otro programa o software malicioso. La política asume que el contenido en intranet será suministrado por una variedad de unidades descentralizadas y que no hay un proceso central de depuración para este mismo contenido. Si se emplea un proceso de depuración central, entonces esta política es innecesaria. La política respalda un depósito de programas probados, autorizados y documentados que se puedan reutilizar repetidamente. Este depósito no debe limitarse a contenido activo, sino que debe incluir una amplia variedad de programas, incluso rutinas de cifrado y extensiones del sistema de control de acceso para soportar la autentificación extendida de usuario.

Políticas Relacionadas: “[Inhabilitación de Java](#)” y “[Ejecución de Programa Java](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

50. Revisión de Páginas Web en Intranet

Política: Todas las páginas web desarrolladas por los usuarios deben pasar una prueba que revele problemas de seguridad y operacionales, según un proceso autorizado por el departamento de Seguridad Informática, antes de ser colocadas en la intranet de la Empresa X.

Comentario: La finalidad de esta política es evitar vulnerabilidades en las páginas web de la intranet desarrolladas por los usuarios, que puedan presentar problemas de seguridad. Otras vulnerabilidades que se pueden detectar mediante dicha revisión incluye el detectar la presencia de virus, la no conformidad con las convenciones organizacionales de formato, el uso de software no autorizado y vínculos rotos. La política deliberadamente evita la mención de estas pruebas porque éstas sufren cambios en el tiempo. El proceso autorizado de prueba se puede cambiar regularmente para reflejar estos nuevos desarrollos, mientras que la política permanece igual.

Políticas Relacionadas: “[Guía de Estilo de Intranet](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

51. Propietario de Información en la Intranet

Política: Toda la información colocada en la intranet de la Empresa X debe tener un Propietario designado, y la información de contacto de este Propietario debe estar claramente indicada en la página donde aparece la información.

Comentario: Esta política insiste en que toda información colocada en intranet debe tener un Propietario designado. Si tal Propietario está identificado, entonces se le puede informar sobre los errores, para que él mismo sea quien autorice la acción correctiva. Este Propietario toma decisiones acerca de la difusión de la información a otros usuarios además de aquéllos que ya tienen acceso. Este Propietario también decide sobre el uso de esta información en otro contexto, tal como el establecimiento de vínculos a la información. Este Propietario a menudo toma las decisiones finales acerca del diseño de las páginas en

intranet. Esta política fomenta los esfuerzos para asignar Propietarios a cada tipo de información interna importante. Normalmente, esta política sólo se distribuye a aquellos responsables por el mantenimiento de páginas web de la intranet.

Políticas Relacionadas: “[Asignación de la Propiedad de la Información](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

52. Firmas Digitales del Propietario de la Información

Política: Todos aquellos Propietarios que coloquen información de la cual son responsables en la intranet de la Empresa X, deben generar firmas digitales que indiquen su autorización en la versión final de las páginas y publicar dichas firmas digitales en conjunción con las páginas.

Comentario: Esta política detecta con facilidad los cambios no autorizados en las páginas intranet. Si las firmas digitales se envían junto a las páginas relacionadas, puede emplearse un sistema de detección de intrusión o algún otro software para determinar automáticamente cualquier cambio no autorizado. La verificación de la existencia de una firma digital válida puede ser parte de un proceso por el cual todas las páginas pasen antes de ser colocadas en la intranet. Esta política asume que se ha puesto en práctica un sistema de cifrado de infraestructura de clave pública (PKI, por sus siglas en inglés). PKI permite cierta flexibilidad sobre este control, incluyendo la firma de más de un Propietario en una página, si éste fuera el caso. En esta política, nada evita la actualización automática a una página intranet. Puesto que un Propietario puede firmar secciones de una página en lugar de la página entera, la parte actualizada de manera automática de una página puede dejarse sin firma. Para reconocer el hecho de que este contenido cambia de manera dinámica, se puede agregar a esta política una oración adicional que indique la autorización del Propietario para un proceso de actualización.

Políticas Relacionadas: “[Ejecución de Programa Java](#)” y “[Protección de Registros del Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

53. Revisión de Datos en Intranet

Política: El departamento de Seguridad Informática deberá revisar trimestralmente todas las colocaciones efectuadas en la intranet de la Empresa X para confirmar que ninguno contiene información confidencial o secreta.

Comentario: Esta política establece un mecanismo para garantizar que los usuarios de intranet no publicarán información con una clasificación más estricta que "sólo para uso interno." Esta política asume que no existe una autoridad central para colocar información en la intranet. Si existiera una autoridad de aprobación centralizada, esta política sería innecesaria porque el filtrado ya se habría realizado. Se recomienda que esta revisión sea realizada por un profesional de seguridad informática, debido a que ellos tienen experiencia en este proceso y pueden fácilmente identificar colocaciones no apropiadas o si ha habido violación de políticas. Esta política asume que la organización ha puesto en práctica un sistema de clasificación de la información.

Políticas Relacionadas: “[Clasificación de Datos en Tres Categorías](#)” y “[Secretos Industriales en la Intranet](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

54. Autorización para Servidor Intranet

Política: Todos los servidores intranet de la Empresa X deben ser autorizados por el administrador de servicios de red del departamento de Sistemas Informáticos antes de conectarse a la red interna.

Comentario: Esta política controla lo que a veces es un proceso aleatorio, en el que varios departamentos establecen sus propios servidores intranet. Algunos sistemas de manejo de redes indican la presencia de máquinas no autorizadas en la red, generando alarma. Se aconseja obtener la autorización del administrador de servicios de red, porque esto ofrece una oportunidad de asegurar que sólo se usan equipos y software normalizados, que el servidor tiene asignada una dirección apropiada en la red y que las demás tareas de configuración se han completado.

Políticas Relacionadas: “[Interconexión de Sistemas](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

55. Acceso a Sistemas de Producción por Intranet

Política: La intranet de la Empresa X no debe usarse para proveer conexiones de tiempo real a ningún sistema de información de producción que tenga controles extendidos de acceso de autenticación de usuario, a menos que se haya obtenido la autorización de la gerencia de Seguridad Informática.

Comentario: La intención de esta política es evitar que los usuarios y otros empleen la intranet como una ruta novedosa y menos compleja para acceder a los sistemas informáticos internos de la Empresa X. Por ejemplo, los sistemas de contabilidad de producción pueden tener un sistema de control de acceso vía contraseñas dinámicas. Si la intranet se usara para acceder este sistema, se podría evitar pasar por el sistema de control de acceso de contraseña dinámico, disminuyendo así las barreras que los usuarios deben salvar para ganar acceso al sistema. La rapidez con que se despliegan los sistemas en intranet puede complicar la capacidad de la gerencia para estar al tanto de todas las conexiones nuevas. Esta política evita que esas conexiones circundén este importante tipo de control de acceso. Para hacer de ésta una política más rigurosa, se puede eliminar la referencia a "controles extendidos de acceso de autenticación de usuario". En su lugar, sólo se haría referencia a cualquier sistema de control de acceso.

Políticas Relacionadas: "Conexiones a Redes Externas en Tiempo Real" e "Interconexión de Sistemas"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

56. Reenvío de Información de Intranet

Política: Los trabajadores no deben enviar a terceros información que aparezca en la intranet, sin obtener autorización de la gerencia apropiada de la Empresa X.

Comentario: Aunque en la intranet se usan herramientas de Internet, como los navegadores, para accesarla, el intercambio libre y abierto de información de Internet no se aplica a una intranet. Esta política notifica a los trabajadores que no deben permitir a terceros no autorizados ganar acceso a la intranet y que no deben compartir información de intranet con terceros sin la autorización apropiada. Una política como ésta evita la divulgación de la información sensible, la información incompleta y la información que puede ser tomada fuera de contexto. Nada de lo mencionado en

esta política evita que una organización convierta una intranet en una "extranet," donde terceros pueden tener el acceso a una intranet.

Políticas Relacionadas: "Diseminación Secundaria de la Información Secreta"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

57. Transferencia a Internet desde Intranet

Política: Los usuarios de la intranet de la Empresa X no deben transferirse directamente a un sitio de Internet sin ser prevenidos con un aviso que les indique que están a punto de ser transferidos a Internet y que se requiere que confirmen que entienden las particularidades de dicha transferencia de red.

Comentario: Esta política define cuándo los usuarios están en la intranet y cuándo en Internet. Es fácil confundir a los usuarios ya que tanto la intranet como Internet se visualizan mediante el mismo programa navegador de red. Los usuarios pueden entonces divulgar información confidencial de la Empresa X de manera accidental, para más tarde descubrir que no estaban, como pensaban, en la intranet. El aviso referido en esta política generalmente debe incluir palabras que le recuerden a los usuarios los peligros de las comunicaciones en Internet. La intención detrás de este proceso de confirmación es exigir que los usuarios entiendan el aviso.

Políticas Relacionadas: "Establecimiento de Enlaces Calientes en Internet" y "Conexiones Directas a Internet"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

58. Guía de Estilo de Intranet

Política: Todos los trabajadores que desarrollen sitios en la intranet deben observar la guía de estilo y usar los recursos encontrados en el Depósito de Recursos para implementación en la intranet.

Comentario: Esta política requiere que todos los desarrolladores de intranet observen la guía de estilo de intranet, donde se definen renuncias legales, maneras para manejar vínculos a otras páginas, plantillas de páginas, gráficos normalizados y otras guías de formato y requisitos de contenido. Este personal debe usar los componentes autorizados que se encuentran en el

Depósito de Recursos para su puesta en práctica en la intranet. Estos recursos típicamente incluyen, sin limitantes, herramientas para establecer interfaces, aplicaciones desarrolladas internamente, gráficos especialmente adaptados y páginas para edición. Sin el uso consistente de estas herramientas y lineamientos, la intranet puede llegar a ser desordenada, de difícil navegación y con un inadecuado nivel de seguridad. Esta política evita el uso de software de suministro externo y no autorizado que pueda incluir defectos no documentados o código malicioso.

Políticas Relacionadas: “Diccionario de Datos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

59. Traslado de Equipos de Computación de Oficinas

Política: Los equipos de computación de oficinas no deben ser trasladados o reubicados sin la previa autorización de la gerencia del departamento pertinente.

Comentario: Esta política evita que los empleados roben los equipos de computación, alegando que están usando el equipo para realizar actividades de negocio, cuando de hecho no es así. Esto también permite mantener el control en cuanto a cambios en el entorno de los sistemas pequeños de la empresa. Esto brinda a la gerencia local la autorización final sobre la ubicación y usos de los equipos de sistemas pequeños en lugar de otorgarla a un departamento de Tecnología Informática centralizado. La mudanza no autorizada de equipos puede causar problemas no previstos tales como problemas de direccionamiento en la red, problemas de cableado eléctrico, riesgos de incendio y problemas de ventilación.

Políticas Relacionadas: “Códigos de Identificación de los Equipos” y “Pases de Propiedad”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

60. Posiciones de las Pantallas de los Computadores

Política: Las pantallas de visualización de todos los computadores personales, las estaciones de trabajo y los terminales de computador utilizados para manejar datos sensibles o valiosos, deben estar ubicadas de tal manera

que no se puedan observar fácilmente desde una ventana, por personas que pasen por un pasillo o por personas que estén en cualquier área pública.

Comentario: Esta política disminuye la posibilidad de que personas no autorizadas puedan obtener información sensible de la pantalla de un computador. En algunos casos de espionaje industrial, se ha observado el uso de telescopios de alta potencia para leer el material visualizado en una pantalla a través de una ventana. Muchas personas obtienen acceso a información sensible o valiosa simplemente por estar cerca de un computador que muestra esta información. Algunas organizaciones pueden extender esta política para incluir los teclados. Si personas no autorizadas pueden ver la actividad en un teclado, están en capacidad de recuperar la información que se ha ingresado. Recientemente, se han visto delincuentes organizados en los aeropuertos utilizando binóculos y videocámaras para robar números de tarjeta de crédito de teléfonos. Para prevenir ese abuso, se puede sugerir a los trabajadores que cubran el teclado con una mano mientras usan la otra para ingresar los números, porque de todos modos la idea es la misma. El efecto positivo de esta política es probablemente la creación de mayor conciencia sobre las personas no autorizadas que andan curioseando a las personas que trabajan con computadores portátiles. Esta política asume que los términos “sensible y valiosa” han sido definidos.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías” y “Viajes con Información Secreta”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

61. Protección Contra la Radiación Electromagnética

Política: Los sistemas de la Empresa X que contengan información secreta deben emplear equipos que cumplan con las normas militares para el control de radiaciones electromagnéticas, y se deben ubicar en recintos cerrados rodeados con malla de alambre u otros materiales de bloqueo de radiación electromagnética, tal como se especifica en dichas normas militares.

Comentario: Esta política se refiere a un problema en buena parte desconocido fuera del mundo militar y diplomático. La radiación electromagnética que generan los equipos de computación y de redes puede ser detectada a grandes distancias y posteriormente convertida a señales legibles. Por ejemplo, la información que aparece en un monitor de computador

puede ser recibida hasta una distancia de casi 300 metros usando equipos relativamente baratos, aun sin existir una línea directa de visión con el monitor comprometido. Las normas militares importantes dependen del país donde sean elaboradas, por lo que no se incluyen en esta política, la cual sólo debe ser aplicada a la información de mayor sensibilidad. Con esta finalidad, más que referirse a "sistemas que contengan información sensible," la política se puede redactar para referirse a "sistemas que contengan una compilación de parámetros de seguridad" que incluyan claves de cifrado, contraseñas y semillas de generadores

de números aleatorios. Por ejemplo, una compañía que procese transacciones de tarjeta de crédito puede aplicar esta política a los computadores que almacenen los números de identificación personal para tarjetas de débito y de crédito.

Políticas Relacionadas: "[Módulos de Hardware para el Proceso de Cifrado](#)" y "[Divulgación de Claves de Cifrado — Controles](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

8.07.06 Sistemas PÚBLICAMENTE Disponibles

1. Uso del Nombre de la Organización

Política: El uso escrito y público del nombre de la Empresa X en material publicado requiere la previa autorización del vicepresidente o del departamento de Relaciones Públicas.

Comentario: Esta política evita que los miembros del grupo de trabajo usen el nombre de la Empresa X para propósitos no autorizados. Los trabajadores pueden tratar de usar el nombre de la organización como una manera de obtener credibilidad adicional para otros fines. El uso no autorizado del nombre de la organización puede llevar a una variedad de problemas, incluyendo la responsabilidad por daños sufridos por terceros por confiar en un respaldo por parte de la organización. Esta política también prohíbe el uso de emisiones masivas de correos electrónicos, contribuciones a salas de charlas de Internet y otras comunicaciones generalizadas si se menciona el nombre de la organización. Los empleados de la empresa pueden participar en tales foros si no hacen mención de que trabajan para la Empresa X. Esta política es un enfoque conservador que refleja gran preocupación por la conservación del buen nombre que disfruta la Empresa X.

Políticas Relacionadas: "[Uso por Parte de Terceros del Nombre de la Organización](#)" y "[Excepción de Responsabilidad en Mensajes Personales en Internet](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

2. Publicidad en Internet

Política: La Empresa X no debe entablar ninguna relación con otra organización con respecto a la publicidad, las referencias o a la generación de clientes potenciales de Internet, si esa organización no ha publicado en Internet una política de privacidad consistente o más estricta que la adoptada por la Empresa X.

Comentario: Esta política especifica que el personal de los departamentos de Ventas, Mercadeo y de Relaciones Públicas debe colocar anuncios o realizar convenios de mercadeo sólo con aquellas empresas que valoran la privacidad en Internet. La política, que puede ser expuesta al público por sí misma, envía un claro mensaje en el sentido de que la Empresa X no hace negocios con organizaciones que no aprecian la privacidad de la información personal. Esto es importante, porque algunas organizaciones de terceros a menudo recogen información personal y la transfieren a la Empresa X. Estas organizaciones de terceros representan o son agentes de la Empresa X en Internet y si la Empresa X ha adoptado una política de privacidad, entonces aquellas organizaciones que la representan en Internet también deben adoptar dicha política de privacidad. Las políticas de privacidad de ambas organizaciones deben ser sustancialmente parecidas. Si éste no es el caso, se debe prestar atención especial para garantizar que la información personal recolectada por el tercero se combine accidentalmente con la base de datos de mercadeo y ventas. La combinación de la información personal recolectada bajo diferentes políticas de privacidad hará difícil aplicar la política asociada o elevará los costos sin necesidad, porque la política de privacidad más estricta debe ser la que domine y se aplique a toda la información. Para aquellas organizaciones que no deseen tomar una decisión sobre si las políticas de privacidad son consistentes, se puede

modificar la última parte de la política para que haga referencia sólo a la política de privacidad publicada. Esta opción es, en gran medida, más frágil y no se recomienda. De manera similar, el alcance de las políticas puede restringirse para que sólo incluya la publicidad y no las referencias o los esfuerzos de generación de prospectos. De manera indirecta, esta política puede prevenir que la organización que emite la política envíe correos electrónicos no solicitados, puesto que las organizaciones que así lo hacen con frecuencia ocultan su identidad y no publican políticas de respeto a la privacidad.

Políticas Relacionadas: ‘‘Avisos Empleados,’’ ‘‘Convenio de Redes con Socios de Negocios,’’ y ‘‘Distribución de Materiales de Mercadeo’’

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Cookies en Internet

Política: Todos los visitantes a los sitios web y sitios de comercio de la Empresa X en Internet deben recibir un aviso indicando la fuente de las "cookies" y "web bugs" usados por esos sitios y su intención.

Comentario: Esta política requiere que el grupo interno de trabajo informe a los usuarios remotos sobre los mecanismos de recopilación de información existentes que emplean "cookies" o "web bugs." Los "cookies" son pequeños archivos de texto que identifican de manera única al usuario, mientras que los "web bugs" son pequeños gráficos insertados en el código HTML que permiten el intercambio de información con el usuario. Tanto los "cookies" como los "web bugs" no pueden ser visualizados por los usuarios, aunque los navegadores más recientes se pueden configurar para preguntar a los usuarios si aceptarían un "cookie" desde un sitio en particular. Mucho sitios web colocan cookies en las máquinas de los usuarios o despliegan "web bugs" a nombre de terceros que se dedican al mercadeo, y dichos "cookies" o "web bugs" se pueden utilizar para informar más adelante sobre las actividades del usuario a medida que navega en la red. Cuando los usuarios saben qué tipo de "cookies" se están empleando y quién las emite, entonces están en posición de decidir si los aceptan o no. Algunos sitios ofrecen una forma alterna de interactuar con el sitio que no requiere aceptar "cookies." Los usuarios no pueden optar inteligentemente por este tipo de interacción a menos que conozcan la naturaleza y el origen de los "cookies" empleados. Cuando los usuarios conocen la naturaleza y origen de los "web bugs" pueden entonces, inteligente-

mente, decidir en qué forma prefieren interactuar con el sitio. Esta política es un indicativo que el patrocinante de un sitio no desea ocultar el uso de "cookies" o de "web bugs", que por ende ayuda a los usuarios a tomar decisiones inteligentes acerca de su relación con el sitio y que quieren hacer negocios en Internet de manera correcta y honesta. El requerir que todos los visitantes sepan como borrar o desactivar "cookies" y "web bugs" puede mejorar aún más esta política.

Políticas Relacionadas: ‘‘Cookies para Inicios Automáticos de Sesión’’ e ‘‘Información Personal Incluida’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Presentación de la Imagen Pública

Política: La Empresa X debe mantener en todo momento una imagen segura y discreta tanto hacia el público como hacia terceros, en relación con cualquier información que se tenga sobre la existencia y naturaleza de bienes importantes, accesibles sólo a aquellas personas que demuestren la necesidad de conocerla.

Comentario: Esta política disminuye las pérdidas potenciales y fomenta la confianza en la Empresa por parte del público y de terceros. Por ejemplo, una organización no debe tener su centro de procesamiento de datos en la planta baja de un edificio en el centro de una ciudad y tener grandes ventanas sin cortinas que den una visión clara del interior a los peatones. Esto representaría una invitación a potenciales saboteadores y espías industriales. Aunque esto parece no ser consistente con la política, ciertos eventos, como un incendio en un edificio de oficinas, se deben notificar al público, puesto que esto los puede afectar. En algunas jurisdicciones e industrias, existen leyes o reglamentos que requieren que se reporten los accidentes. Aunque se admite un evento relativo a seguridad, las medidas de control para evitar futuros eventos se deben mantener confidenciales. Esta política y las aclaratorias anexas pueden resultar un trasfondo particularmente útil para el departamento de Relaciones Públicas, cuando se hagan declaraciones que describan eventos con pérdidas. Una decisión difícil es asumir que una imagen buena y segura es un mejor objetivo que disuadir a otros en el uso de las mismas técnicas.

Políticas Relacionadas: ‘‘Notas de Prensa Sobre Información de Vulnerabilidad’’ y ‘‘Divulgación de las Vulnerabilidades del Sistema Informático’’

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

5. Secretos Industriales en la Intranet

Política: Todos los secretos industriales de la Empresa X son identificados por el jefe del grupo legal y se deben listar y describir en forma breve en la intranet.

Comentario: Esta política notifica a los trabajadores que la información de la Empresa X identificada como secreto industrial debe contar con una protección especial. Antes de pensar que los trabajadores vayan a tratar dicha información con previsiones especiales de seguridad, éstos deben saber a qué información hay que darle dicho tratamiento. Una forma de lograr esto, es con una página intranet en la que se listen los secretos industriales sin explicar los detalles. La preparación y la actualización habitual de una lista de secretos industriales puede ser un indicativo de que la gerencia ha tomado en serio la protección de estos tipos de información y de que un tribunal debería emitir una protección especial en cuanto a secretos industriales, de ocurrir un proceso legal. Se debe controlar el acceso a la intranet para impedir el acceso de terceros no autorizados en busca de objetivos de interés. Se debería utilizar también una etiqueta de clasificación de datos para secretos industriales. En este caso, sería apropiada la denominación "máxima seguridad". El publicar una lista de secretos industriales a una intranet no elimina la necesidad de las etiquetas. Se debe obtener asesoría legal antes de adoptar una política como ésta.

Políticas Relacionadas:“[Divulgación de Secretos Industriales por Internet](#)” y “[Software Distribuido a Terceros](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Medianos y altos

6. Servicios Telefónicos en Internet

Política: Nno deben utilizarse los servicios telefónicos de Internet para la transmisión de información secreta no cifrada de la Empresa X.

Comentario: Esta política alienta a los usuarios que quieran emplear los servicios telefónicos en Internet, a tomar en cuenta la naturaleza de la información a ser transmitida y de ser necesario, transmitir información secreta mediante otros canales más seguros. Se hacen cada vez más populares los servicios de teléfono vía Internet debido a su bajo costo. Sin embargo, las conversaciones que viajan por este medio se envían a través de máquinas administradas por personas que pueden o no estar monitoreando la transmisión. Estas transmisiones se pueden grabar y luego revisar si las identidades u otras circunstancias de los interlocutores parecen interesantes. Esta política asume que la palabra "secreta" ha sido claramente definida en otro sitio, generalmente en una política de clasificación de información.

Políticas Relacionadas:“[Conversaciones Telefónicas Sobre Información Sensible](#)” y “[Monitoreo o Grabación de Conversaciones Telefónicas](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Medianos y altos

7. Estaciones de Trabajo de Acceso Público

Política: Todos los archivos suministrados por los usuarios y todos los archivos temporales creados por software residente en las estaciones de trabajo, deben ser borrados automáticamente al final de la jornada de trabajo.

Comentario: Esta política evita que los archivos colocados en una estación de trabajo con acceso público sean accidentalmente divulgados a otros usuarios distintos a los que colocaron dichos archivos en esa estación de trabajo. La política también evita la contaminación de la estación por virus y gusanos insertos en archivos que otro usuario colocó en esa estación de trabajo con acceso público. Siempre es posible que un usuario emplee un programa de servicio de disco para recuperar archivos borrados de otros usuarios, con el objetivo de evadir esta política. Si los archivos son confidenciales, entonces el usuario comprometido nunca deberá colocarlos en una estación de trabajo de acceso público.

Políticas Relacionadas:“[Directorios Modificables por el Público](#)” y “[Revisión de la Información Respaldada](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Bajo

8. Identidades Falsas

Política: Los trabajadores no deben tergiversar, ocultar, suprimir o reemplazar su identidad en ninguna comunicación electrónica.

Comentario: Esta política notifica a los usuarios que bajo ninguna circunstancia pueden tergiversar su identidad en los sistemas electrónicos de comunicación. El alcance de la política es deliberadamente amplio e incluye sistemas telefónicos y sistemas de correo electrónico. Un ejemplo de una acción prohibida por esta política es la extracción de partes del texto de un mensaje de correo electrónico, para después incorporarlo dentro de otro mensaje de correo electrónico, sin dar crédito a su creador. Esta política no requiere que toda la información de ruta de un mensaje de correo electrónico se mantenga, sólo la identidad del creador. De conformidad con esta política, el uso del identificador de usuario de otra persona representa una violación de la política. Esta política asume que no existen identificadores de usuarios asignados a grupos, exigiendo que cada usuario tenga un identificador individual de usuario.

Políticas Relacionadas: "Representaciones de la Organización," "Atribución de la Información," y "Representaciones en Internet Que Incluyan Afiliación"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Validación Cruzada de la Información

Política: La información importante de la cual dependa la gerencia debe ser comparada periódicamente con fuentes externas validadas y de manera cruzada, para asegurar que es una representación precisa de la realidad.

Comentario: Esta política valida la información importante para asegurar que es un reflejo de la realidad. La integridad de la información tiene sentido sólo si se compara periódicamente con la fuente independiente o externa. Un ejemplo implica cifras de inventario mantenidas en un computador; si estas cifras no son periódicamente conciliadas con las cifras actuales, disminuye su integridad. La frecuencia de la validación cruzada variará de acuerdo con el tipo de información

en referencia. Si se habla del valor de las acciones que se cotizan en la bolsa, "periódicamente" significa cada día bursátil. Si se refiere a la condición médica de un grupo en un puesto de confianza, entonces "periódicamente" implica anualmente.

Políticas Relacionadas: "Revisión de Análisis Computarizados" y "Validación de los Controles"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Sin Responsabilidad en Mensajes

Política: Un mensaje de renuncia debe colocarse en todos los sitios de la red donde la Empresa X esté actuando como un transportista común, indicando que la empresa no controla el contenido de los mensajes en el sitio, no verifica la corrección, la exactitud o la validez de la información que aparece en el sitio y no es responsable del contenido de ningún mensaje que aparezca en el sitio.

Comentario: Históricamente, se han presentado muchos conflictos legales asociados a la responsabilidad de los operadores de sistemas de foros electrónicos (BBS, por sus siglas en inglés), en cuanto a las actividades ilegales que ocurren en su BBS de acceso telefónico. Estas mismas consideraciones se aplican a sitios en la red, en Internet o en cualquier otro foro electrónico donde interactúan terceros. Esta política coloca a la Empresa X en una posición donde no se hace responsable por estas actividades, tal como la compañía telefónica no se hace responsable por actos ilegales que otros realizan en sus sistemas. Con esta política, el operador del sistema censura o suprime mensajes. Aunque otras doctrinas legales forzarán a una organización a responsabilizarse de los actos de sus empleados, esta política disminuye la exposición de la Empresa X a mensajes publicados en sus sistemas. Es importante revisar esta política con el grupo legal interno. La palabra "sitio" en la política implica que este mensaje de renuncia le será presentado a la gente cuando entren al sitio.

Políticas Relacionadas: "Comentarios Públicos en Sistemas Electrónicos," "Excepción de Responsabilidad en Mensajes Personales en Internet," "Excepciones de Responsabilidad por Daños a Datos y Programas," y "Normas de Telefónicas Comunes"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Mensajes de Delincuentes o Terroristas

Política: Los mensajes emitidos por delincuentes o terroristas no deben ser retransmitidos en canales públicos empleando los sistemas informáticos de la Empresa X.

Comentario: Esta política evita que delincuentes y terroristas usen canales de retransmisión públicos como vía para popularizar sus causas. El retransmitir estos mensajes sería similar a permitir que un enemigo usara un sistema de radio o TV como canal clandestino. Esta política estará en desacuerdo con los objetivos de ciertas personas de mercadeo que creen que el retransmitir dichos mensajes es una manera de aumentar las ganancias. Esta representa una política de seguridad pública en conjunción con una política de seguridad informática. Un resumen conciso o un análisis del mensaje se puede retransmitir después de obtener la autorización de la gerencia. Para que el delinquente o el terrorista no obtenga mayor fama personal o notoriedad, es conveniente que no se transmitan ni fotos del individuo, ni películas que lo involucren directamente.

Políticas Relacionadas: “[Derecho a la Libre Expresión](#)” y “[Transmisiones a Través de Correo Electrónico y Correo de Voz](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

12. Comentarios Públicos en Sistemas Electrónicos

Política: Los comentarios no oficiales que los trabajadores publiquen en un sistema de correo electrónico, en foros electrónicos o en otros sistemas electrónicos, no se deben entender como la posición oficial o declaraciones formales de la Empresa X.

Comentario: Esta política notifica a los usuarios que no deben asumir automáticamente que lo que leen u observan en los sistemas de la Empresa X es necesariamente política de la Empresa X. En su lugar, deben buscar pruebas de que el material es lo establecido por una política. Otra finalidad de esta política es notificar a los usuarios que lo que leen u observan puede ser eliminado en el corto plazo. La política notifica a los usuarios que la organización no se verá limitada por estas declaraciones, ni garantiza que las mismas sean correctas o autorizadas. Esta posición es válida dada la facilidad con la cual la mayoría de los mensajes del correo electrónico pueden ser simulados. Aunque la política está orientada hacia los sistemas informáticos tales como Internet y los foros electrónicos, pueden

incluirse el correo de voz y otros sistemas de comunicaciones. Se puede suprimir de la política la mención específica del tipo de sistema, haciendo referencia en su lugar a “sistemas electrónicos de comunicaciones.” Esta política es el equivalente a las declaraciones ofrecidas por muchas estaciones de TV y radio que dicen, “las opiniones aquí expresadas no son necesariamente las de la estación o las de la gerencia de la estación”.

Políticas Relacionadas: “[Sin Responsabilidad en Mensajes](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

13. Etiquetas de Contenido en Internet

Política: Toda la información publicada en los sitios de comercio y de red de la Empresa X, se debe acompañar por etiquetas de contenido normalizado.

Comentario: Esta política ayuda a la organización que publica contenido en Internet a evitar la mala publicidad, las quejas y otros problemas. Los usuarios pueden emplear software de investigación de contenido para impedir la divulgación de material específico. Los patronos pueden usar software de revisión de contenido tal como el que se usa en los cortafuegos, para limitar el acceso del empleado a un material específico. El etiquetado del contenido ayudará a los usuarios y a los patronos en sus esfuerzos por limitar un acceso o una exhibición de la información no deseada. A pesar de que es conveniente que la organización que publique el material haga también el etiquetado, estas organizaciones deben estar al tanto de que los terceros hacen independientemente su propia clasificación.

Políticas Relacionadas: “[Censura de Datos](#)” y “[Comunicaciones Potencialmente Ofensivas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

14. Grupos de Discusión en Internet

Política: Los usuarios no deben usar sus identificadores de usuario de la Empresa X, para publicar contenido en línea conjuntamente con grupos de discusión polémicos en Internet o en otro foro público.

Comentario: Esta política evita que la Empresa X se haga involuntariamente blanco de cualquier grupo que se ofenda por una publicación en un foro público. El tercero ofendido puede lanzar un ataque para tomar

represalias que serían contraproducentes para las operaciones de la organización. Esta política no restringe la libertad de los usuarios para expresarse en línea, sólo estipula que ninguna publicación personal se debe iniciar con el identificador de usuario emitido por la Empresa X.

Políticas Relacionadas: “Discusiones Utilizando Servicios Computacionales y Comunicacionales” y “Derecho a la Libre Expresión”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Comunicaciones Salientes en Internet

Política: Todas las comunicaciones salientes en Internet deben respetar la reputación de la Empresa X y su imagen pública.

Comentario: Esta política está concebida para evitar complicaciones legales y también para asegurarse de que los trabajadores no pongan en ridículo a una organización en Internet por descuido. La política dicta cierta norma de profesionalismo y decoro que los trabajadores constantemente deben seguir. La política proporciona la base para amonestar o hasta despedir al trabajador que hizo quedar mal a la organización en un foro público.

Políticas Relacionadas: “Remoción de Material Ofensivo” y “Avisos Públicos Inadecuados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

16. Términos y Condiciones en Internet

Política: Se debe suministrar a todos los clientes que usen Internet para la colocación de órdenes, un resumen de los términos y condiciones de la Empresa X, y para poder completar sus órdenes deben indicar específicamente que están de acuerdo y supeditados a dichos términos y condiciones.

Comentario: La intención de esta política es establecer con exactitud la manera de ejecutar en Internet un arreglo o venta entre dos partes interesadas. Lo que motiva la necesidad de tener esta política es el hecho de que Internet pasa por distintas jurisdicciones con distintas leyes acerca de los contratos de negocios. En estos casos, no están claras ni la jurisdicción correspondiente ni las leyes aplicables. La política requiere que un cliente haga click con el ratón en el botón que dice “Estoy de Acuerdo”, o que utilice cualquier otro mecanismo comparable con el fin de demostrar claramente que entendió y estuvo de acuerdo con los términos y condiciones de la Empresa X. Dichas indicaciones por parte del cliente se pueden considerar iguales a su firma autógrafa. En muchas jurisdicciones no se ha determinado la base legal de este acuerdo electrónico.

Políticas Relacionadas: “Contratos Obligatorios en Sistemas Electrónicos” y “Convenio de Redes con Socios de Negocios”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Capacidades del Explorador del Correo Electrónico

Política: Las opciones de correo electrónico presentes en los programas navegadores de Internet no se deben utilizar para ninguna comunicación del negocio.

Comentario: Esta política evita que los usuarios empleen las opciones de correo electrónico del navegador, puesto que emplearlas elude los controles incluidos en los sistemas internos de correo electrónico. Si los usuarios emplean un navegador para el correo electrónico, especialmente si se conectan vía su proveedor de servicio personal con una línea de conexión telefónica, pueden descargar un anexo que contenga virus. Si este anexo del correo electrónico hubiera pasado en su lugar por el servidor normal de correo electrónico de la organización, habría podido ser filtrado y suprimido, evitando cualquier daño. El uso de un navegador para el correo electrónico puede evitar sistemas de registro del encabezado del correo electrónico y sistemas de revisión de contenido. Esta política también evita que los trabajadores ofrezcan a los clientes y a los clientes potenciales sus direcciones personales del correo electrónico, si consideran que el sistema interno del correo electrónico es demasiado lento o pesado.

Políticas Relacionadas: “[Monitoreo de Mensajes de Correo Electrónico](#)” y “[Retención de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Fuentes de Noticias en Internet

Política: Los avances noticiosos, las listas enviadas por correo electrónico, las actualizaciones de datos iniciadas por terceros y otros mecanismos de recepción de información en Internet, deben restringirse al material claramente relacionado con el negocio de la Empresa X y a las tareas de los trabajadores que lo reciben.

Comentario: La finalidad de esta política es informar a los administradores del sistema que deben filtrar los avances noticiosos en Internet de tal manera que sólo el material comercial llegue a los trabajadores de la compañía. Esta política también brinda a la gerencia de manera implícita, el derecho a examinar el correo electrónico y las actualizaciones iniciadas por terceros, para determinar no sólo si el material está relacionado con el negocio, sino también si está relacionado con las tareas del trabajador que lo recibe. En algunos casos, la

política se puede emitir también a los usuarios, actuando en efecto como respuesta a solicitudes de avances noticiosos y otros servicios informativos. La política evita que las discusiones sobre avances noticiosos de asuntos ajenos al negocio distraigan al personal interno. La política también ayuda a conservar el espacio en disco y otros recursos del sistema tales como el ancho de banda en la red. La política asume que los usuarios no usan conexiones telefónicas para acceder a Internet, sino que pasan a través de un cortafuego interno, de un servidor de correo interno y otros sistemas relacionados. Si los usuarios usan conexiones telefónicas para acceder a Internet, las decisiones sobre los avances noticiosos las tomará un proveedor de acceso de Internet y los usuarios relacionados.

Políticas Relacionadas: “[Conexiones a Redes Externas en Tiempo Real](#)” y “[Uso Personal de los Servicios de Internet de la Organización](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

19. Modificación de Información por Internet

Política: Los usuarios que se conectan con los sistemas de la Empresa X a través de Internet no deben modificar directamente ninguna información de la Empresa X.

Comentario: Esta política refleja la evolución de las instalaciones de seguridad en Internet y las preocupaciones que muchos administradores tienen sobre la falta de seguridad. La política cuida la integridad de los registros internos mediante un procedimiento de revisión. Al seguir esta política, los usuarios conectados a Internet pueden solicitar actualizaciones de los registros internos, pero estas peticiones deben ser revisadas por una persona o un proceso automatizado antes de ser colocados en cualquier almacén de información de producción de la Empresa X, tales como las bases de datos, los diccionarios de datos, los archivos principales y las páginas en la red. Utilizando mecanismos sólidos de autenticación del usuario, tales como contraseñas dinámicas y sistemas complejos de cifrado, la modificación de los expedientes internos a través de Internet puede hacerse de manera segura. De adoptarse esta política, puede sufrir modificaciones en el futuro, a medida que evolucionen las instalaciones electrónicas de comercio basadas en Internet. Por ejemplo una definición de “modificación directa” puede ser una “actualización en tiempo real basada en la información proporcionada por el usuario sin verificaciones de racionalidad”.

Políticas Relacionadas: “Actualización de Información de Producción” y “Autorización para Transacciones de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

20. Excepción de Responsabilidad en Mensajes Personales en Internet

Política: Cada vez que un trabajador publique un mensaje a un grupo de discusión en Internet, a un foro electrónico o a otro sistema de información pública sin la autorización previa del departamento de relaciones públicas, este mensaje debe estar acompañado por una frase que especifique claramente que estos comentarios no representan necesariamente la posición de la Empresa X.

Comentario: Esta política blinda a la Empresa X contra demandas por libelo, demandas de infracción de derechos de autor, la divulgación no autorizada de secretos industriales u otros problemas que se presentan cuando uno de sus trabajadores hace una colocación en un sistema de información público. Tales renuncias son necesarias incluso si el nombre de la organización no aparece en el texto del mensaje. Varias porciones de la información pueden poner en evidencia a la organización involucrada, tales como la naturaleza de los comentarios hechos, la dirección del correo electrónico indicado o el nombre del individuo.

Políticas Relacionadas: “Sin Responsabilidad en Mensajes,” “Pie de Página de Correo Electrónico Saliente,” y “Comentarios Públicos en Sistemas Electrónicos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

21. Representaciones en Internet Que Incluyan Afiliación

Política: Al participar en grupos de discusión, en salas de charla y en otros servicios en Internet, sólo los individuos autorizados por la administración para proporcionar apoyo oficial a productos y servicios de Empresa X, pueden indicar su afiliación con la Empresa X.

Comentario: Esta norma limita el número de representantes oficiales de la Empresa X en Internet, lo cual disminuirá las oportunidades de libelo, de difamación, de tergiversación y de problemas judiciales parecidos. Las organizaciones que adopten esta norma pueden además exigir que los trabajadores que los representan en Internet estén adiestrados en relaciones públicas. Un área que puede necesitar mayor explicación es la relacionada con las declaraciones oficiales, tales como las ofrecidas a la prensa. Sin embargo, en la mayoría de los casos, palabras tales como “a menos que se haya estipulado lo contrario” cubrirán estos casos.

Políticas Relacionadas: “Excepción de Responsabilidad en Mensajes Personales en Internet” y “Comentarios Públicos en Sistemas Electrónicos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

22. Representaciones en Internet de Productos y Servicios

Política: Los trabajadores no deben anunciar, promover, presentar ni hacer declaraciones acerca de los productos y los servicios de la Empresa X en foros de Internet, tales como listas de correo, grupos de noticias o salas de charlas, sin la previa autorización de los departamentos de Ventas y Relaciones Públicas.

Comentario: Esta norma controla lo que los trabajadores dicen acerca de los productos y los servicios de la Empresa X. Esta norma garantiza que las representaciones públicas serán sólidas y un reflejo de las intenciones de la gerencia. Las facilidades de comunicación proporcionadas por Internet son de gran alcance y las mismas deben controlarse cuidadosamente para evitar problemas legales, tales como el libelo y la difamación. En muchos casos, los trabajadores tienen buenas intenciones, con la esperanza de ayudar a su patrón, pero el efecto global puede ser bastante diferente. Esta norma permite que la organización adiestre gente seleccionada para controlar en forma habitual estos foros y responda tal como el hilo de discusión lo requiera.

Políticas Relacionadas: “Foros Electrónicos Públicos,” “Comunicaciones Públicas,” y “Liberación de Información de la Organización”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

23. Divulgación en Internet de Información de Contacto

Política: Tanto niños como adultos no deben revelar sus nombres verdaderos, sus direcciones, ni sus números de teléfono en foros electrónicos, en salas de charla ni en otros foros públicos en Internet.

Comentario: Esta norma está dirigida a evitar que los niños y los adultos preocupados por las situaciones de acecho, acoso u otras invasiones de su intimidad, se vean molestados innecesariamente. Esta norma, que está destinada a ser ofrecida como servicio público para el uso personal en Internet, resulta poco práctica para la mayoría de las actividades de negocios en Internet, porque los interesados necesitan intercambiar dinero o artículos físicos, en cuyo caso la información de contacto se debe suministrar obligatoriamente. La política notifica a la gente que puede ocultar su identidad y que no necesita revelar tal información cuando estén en línea. La política es muy importante para al uso de Internet fuera de horas de trabajo. Las organizaciones que dan esta política a sus usuarios o sus clientes, pueden también incluir instrucciones que incluyan que los niños no deben responder a mensajes que consideren sugestivos, beligerantes o que los hagan sentir incómodos. Los niños no deben realizar reuniones personales con otros usuarios sin consentimiento parental previo. Los padres pueden considerar la instalación de software que pueda controlar el contenido de las sesiones en Internet y de software que pueda bloquear el acceso a ciertos sitios en Internet que contengan material inadecuado. Las organizaciones que asumen un enfoque proactivo frente a estos potenciales problemas con los niños de sus empleados, reducirán los problemas personales que puedan eventualmente interferir con el desempeño del empleado.

Políticas Relacionadas: “[Privacidad en Correo Electrónico](#)” y “[Validación de la Identidad de Terceros](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

24. Declaraciones Políticas y Patrocinio de Productos o Servicios

Política: Los trabajadores no deben realizar declaración política alguna de defensa o endoso a productos o servicios que indique afiliación con la Empresa X, a menos que hayan obtenido permiso del departamento de Relaciones Públicas.

Comentario: Las salas de charla, los grupos de noticias y el correo electrónico dan a los usuarios de Internet una oportunidad sin precedentes de contactar a otros usuarios. Esta política garantiza que tal comunicación se utilizará de manera que fomente los intereses de la organización y que no cree problemas legales o de relaciones públicas. Esta política de ninguna manera evita que los usuarios de Internet hagan declaraciones prohibidas en su rol de individuos, sin ninguna afiliación a la Empresa X usando una dirección personal de correo electrónico y otras instalaciones no pertenecientes a la Empresa X. Algunas organizaciones querrán que el departamento legal quedase a cargo de realizar la mencionada autorización, en lugar del departamento de Relaciones Públicas.

Políticas Relacionadas: “[Representaciones en Internet Que Incluyan Afiliación](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

25. Divulgación de Secretos Industriales por Internet

Política: La participación en grupos de discusión, salas de charla y otros foros públicos en Internet, relacionados con los negocios de la Empresa X, deben restringirse a los trabajadores designados que han sido instruidos sobre la divulgación de secretos industriales.

Comentario: Esta política evita la divulgación accidental de los secretos industriales en foros públicos, tales como los grupos de discusión en Internet. A menudo, empleados bien intencionados participan en discusiones y sólo después se dan cuenta que han divulgado algo confidencial o patentado. Esta política no hace mención deliberada acerca de la participación en foros públicos sobre asuntos no relacionados con el negocio de la Empresa X. El alcance de la política se puede ampliar para incluir salas de charla en Internet.

Políticas Relacionadas: “[Representaciones en Internet Que Incluyan Afiliación](#),” “[Sin Responsabilidad en Mensajes](#),” y “[Divulgación de Secretos Industriales](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

26. Preguntas sobre Seguridad en Internet

Política: Las consultas sobre la seguridad de los computadores o de las redes, no deben publicarse en grupos de noticias de Internet o en ningún otro foro público.

Comentario: Esta política mantiene un bajo perfil en cuanto a los problemas de seguridad que se pueden presentar en la Empresa X. La discusión sobre las debilidades que existen en el sistema de la Empresa X invita a críticas de terceros y hasta ataques para explotar dichas vulnerabilidades. En muchos casos, el personal técnico bien intencionado desconoce la manera de resolver ciertos problemas de seguridad de la información, y a menudo buscan las respuestas en Internet. Esta política permite la búsqueda de respuestas en Internet, pero no permite publicar cualquier indicación del estado actual de los sistemas en la Empresa X. La política motiva al personal técnico a consultar al departamento de Seguridad Informática o a un consultor externo de seguridad informática. La política se puede modificar para permitir las publicaciones anónimas, en cuyo caso la identidad de la Empresa X no se hace evidente, pero esta política es mucho más simple y evita los pasos a tomar para lograr un verdadero anonimato en Internet.

Políticas Relacionadas: “Divulgación de Ataques a Sistemas de Computación” y “Divulgación en Internet de Información de Contacto”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

27. Transmisión por Internet de Información Sensible

Política: No se debe enviar vía Internet la información no cifrada, secreta, patentada o privada de La Empresa X .

Comentario: Esta política informa a los usuarios que, en condiciones normales, la información en Internet no cuenta con protección automática. Esta política garantiza que el cifrado se usará para toda información sensible enviada vía Internet. En última instancia y como caso base, muchas redes incorporarán facilidades de cifrado, pero mientras tanto, será necesario que los usuarios se encarguen del proceso de cifrado. El código fuente es especialmente privado y necesita ser reconocido como tal por muchas organizaciones. Esta política es la más conveniente para organizaciones tales como compañías de teléfono y empresas de software, que generan su propio código fuente.

Políticas Relacionadas: “Cifrado de Correo Electrónico,” “Seguridad de la Información Sensible,” “Gestión Automática de Claves de Cifrado,” y “Envío de Información Secreta Vía Fax — Cifrado”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

28. Avisos Públicos Inadecuados

Política: El correo electrónico enviado por los trabajadores de la Empresa X a los grupos de discusión en Internet, a foros electrónicos u otros foros públicos, debe ser eliminado si se determina que es opuesto a los intereses de los negocios de la Empresa X o a la política existente en la compañía, dictada por la gerencia de Seguridad Informática o la gerencia de Recursos Humanos.

Comentario: La finalidad de esta política es notificar a los empleados que sus publicaciones públicas pueden ser censuradas si son contrarias a los intereses o políticas de los negocios de la Empresa X. Esta política intenta hacer que los empleados sean más cuidadosos con lo que publican. La política también otorga a la Empresa X el derecho de suprimir rápidamente publicaciones inadecuadas sin un proceso de decisión formal y sin tener que aceptar objeciones. Algunas organizaciones pueden cambiar ligeramente la política para especificar que si los individuos no hacen evidente su afiliación con la Empresa X, incluyendo la afiliación que otorga su dirección del correo electrónico, la Empresa X no tendría ningún derecho de censurar sus mensajes. Una excepción recomendable a esta restricción viene representada por los mensajes relacionados con las actividades económicas de la Empresa X. Por ejemplo, si un representante de servicios al cliente de la Empresa X hizo una declaración personal en un foro público de Internet, dando mala imagen de la Empresa X, a pesar de que no se pueda demostrar afiliación alguna del individuo con la Empresa, ésta puede suprimir ese mensaje. La capacidad de suprimir los mensajes enviados por otros será cada vez más difícil a medida que se usen más las firmas digitales, las rutinas de cifrado y los controles de acceso. En muchos de estos casos, un patrón puede solicitar la eliminación del mensaje vía el encargado del sistema o del proveedor del servicio. La existencia de una política como ésta puede facilitar acuerdos de eliminación del mensaje entre la gerencia de la Empresa X y el operador de sistema implicado. Los derechos legales de la Empresa X al suprimir el derecho individual a la libre expresión pueden ser un problema aquí y deben discutirse con el grupo de consultoría legal.

Políticas Relacionadas: “Censura de Datos,” “Sin Responsabilidad en Mensajes,” y “Normas de Telefónicas Comunes”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

29. Sitios Web Con Nombres Similares

Política: El personal del departamento jurídico de la Empresa X debe emplear periódicamente los sistemas de búsqueda disponibles en la red para determinar si algunos sitios en la red están utilizando nombres similares, con el propósito de simular los sitios autorizados o patrocinados por la Empresa X.

Comentario: Esta política garantiza que un integrante interno del personal, típicamente del departamento jurídico, utilizará los sistemas de búsqueda para identificar sitios potencialmente confusos que puedan utilizar un nombre similar. Esta política informa al personal interno que deben buscar tales sitios falsificados y cuando se detecte uno, notificar al personal apropiado, por lo general, el consultor general. Esta política sería utilizada sólo por los sitios comerciales en Internet preocupados por las amenazas de fraude u otros sitios que estén preocupados de que su buen nombre se vea perjudicado por un sitio web no autorizado.

Políticas Relacionadas: “Monitoreo en Internet del Uso de la Información” y “Páginas Web No Oficiales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

30. Publicación en Internet de Material

Política: Los usuarios no deben colocar material de la Empresa X en ningún sistema informático accesible al público en Internet, incluyendo, sin limitantes, software, notas internas y declaraciones de prensa, a menos que dicha publicación esté autorizada por la gerencia de Relaciones Públicas.

Comentario: Esta política notifica a los trabajadores que no se permite divulgar información a terceros a través de Internet a menos que dicha acción esté autorizada por Relaciones Públicas. Una política como ésta, por ejemplo, otorga a una organización de desarrollo de software la suficiente justificación para despedir a un empleado que publicó copias de un nuevo software en Internet días antes de que el software fuera

lanzado oficialmente. Muchos usuarios de Internet creen que dicha información debe ser compartida. Esta política notifica explícitamente no actuar de acuerdo con esa filosofía. Esta política se puede ampliar para incluir otros ejemplos, tales como los clientes potenciales, la información sobre la calidad de los productos e información de negociaciones con los sindicatos. Para motivar el acatamiento de esta política, una explicación anexa puede hacer referencia a posibles problemas de libelo o difamación y a las fluctuaciones del precio de las acciones de la Empresa X.

Políticas Relacionadas: “Avisos Pùblicos Inadecuados,” “Aprobación de las Representaciones Pùblicas,” “Páginas Web No Oficiales,” “Representaciones de la Organización,” y “Comunicaciones Pùblicas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

31. Acuerdos de Negocios por Internet

Política: Los trabajadores no deben utilizar conexiones de Internet para establecer canales de negocios nuevos o diferentes, a menos que el director de Tecnología Informática y el director de asesoría legal lo hayan autorizado previamente.

Comentario: Esta política detiene iniciativas internas para desarrollar negocios a través de Internet hasta que su seguridad esté garantizada. Puesto que las medidas normales de seguridad para tales acuerdos no están definidas, es crítico que el personal interno examine la seguridad de tales arreglos antes de que la Empresa X active los sistemas de producción. Aunque ciertas asociaciones comerciales especializadas en negocios en Internet se han desarrollado recientemente, la mayoría de las organizaciones todavía no han definido los controles esenciales para las transacciones de negocios en Internet. El documento que contiene estas ideas esenciales de control se conoce generalmente como arquitectura de la seguridad. Se requiere una autorización anticipada por parte de los encargados identificados en la política.

Políticas Relacionadas: “Contratos Obligatorios en Sistemas Electrónicos” y “Convenio de Redes con Socios de Negocios”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

32. Publicaciones en Redes

Política: Los trabajadores deben estructurar correctamente los comentarios y las preguntas que publiquen en foros electrónicos, listas de correo electrónico, grupos de noticias en línea y otros foros públicos, evitando así la divulgación de cualquier información que pueda revelar datos sobre proyectos secretos, proyectos de productos de software por anunciar, proyectos de investigación y desarrollo o asuntos sensibles relacionados de la Empresa X.

Comentario: Esta política está dirigida a sensibilizar a los trabajadores de la Empresa X sobre posteos en sistemas electrónicos públicos. La política puede parecer un nuevo planteamiento de sentido común. Sin embargo, se recomienda notificarla explícitamente a los trabajadores de la Empresa X para propósitos disciplinarios y legales. Internet y los demás foros públicos pueden representar una novedad para algunos usuarios y tal vez no sepan diferenciar las redes internas de las externas. Esta política sirve para recordarles la importancia de esta distinción.

Políticas Relacionadas: “[Acuerdos de Confidencialidad](#)” y “[Responsabilidad en la Seguridad Informática](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

33. Transferencia de Archivos Descargados

Política: Para descargar cualquier archivo de Internet se deben usar computadores que no estén conectados a la red de la Empresa X y estos archivos se deben revisar con un paquete autorizado para detección de virus antes de ser transferidos a cualquier otro computador.

Comentario: Esta política está orientada a evitar que virus, caballos de Troya, gusanos y demás códigos maliciosos se propaguen a través de la red de computadores internos. Esta política permite libre acceso a Internet, pero solamente desde aquellos computadores personales aislados de otras máquinas internas. En algunos casos se necesitarán instrucciones específicas que indiquen cómo aislar un computador personal. Esta política exige que se revisen todos los archivos descargados, para saber si tienen virus antes de transferirlos a otra máquina. La política no se limita a software que reconoce la existencia de virus de macros. La política también hace énfasis en el papel que las redes y su interconectividad juegan en la propagación de los virus.

Políticas Relacionadas: “[Exploración de Software Descargado](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Alto

34. Confiabilidad de la Información de Internet

Política: Toda la información disponible de Internet debe estar bajo sospecha hasta que sea validada por otra fuente.

Comentario: Esta política informa a los trabajadores que mucha de la información disponible en Internet no es confiable. Los trabajadores creen que lo que leen en Internet es digno de confianza. La Internet no está regulada ni supervisada. Esta política define expectativas apropiadas con respecto a la calidad de la información proporcionada vía Internet. Un efecto secundario positivo de esta política es que motiva al personal a pensar profundamente sobre la calidad de la información que se utiliza en la toma de decisiones. La política se puede ampliar para incluir una prohibición de la actualización de registros de la Empresa X con información de Internet hasta que ésta sea confirmada por otra fuente.

Políticas Relacionadas: “[Esconder Transmisión de la Información](#)” y “[Calidad de los Medios de Almacenamiento de Archivos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

35. Carga de Software

Política: Los usuarios no deben cargar software que haya sido licenciado por terceros o software que haya sido desarrollado por la Empresa X, a ningún computador a través de Internet a menos que se haya obtenido la autorización del gerente supervisor del usuario.

Comentario: La distribución no autorizada de software con derecho de autor vía Internet viola la protección de la propiedad intelectual perteneciente a otras organizaciones. Esta política informa a los usuarios que la carga de cualquier software está prohibido a menos que se tenga la autorización de un gerente. Dado que éste es un asunto de gerencia informática relacionado con el usuario, más que un asunto técnico, la gerencia que autoriza es la del departamento y no la gerencia de seguridad informática. La política va más allá del software licenciado, incluyendo el software que se ha desarrollado localmente. La política puede incluir el

software que ha sido confiado a la Empresa X y que quizás no haya sido licenciado. La política evita la distribución no autorizada del software que puede ser secreto industrial o simplemente crítico para la Empresa X. Puesto que es tan fácil para los usuarios transferir archivos vía Internet, son necesarias las políticas explícitas que eviten estas actividades de carga. Una extensión a esta política prohibiría la transferencia del software de un computador a otro, sin importar el sistema de comunicaciones utilizado.

Políticas Relacionadas:“[Descarga de Software](#)” e “[Información Descargada](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

36. Información No Solicitada en Internet

Política: Cualquier mecanismo que reciba comentarios o sugerencias de Internet, tal como está previsto en los sitios de la red de la Empresa X, debe estar acompañado por la siguiente excepción de responsabilidad: "La admisión por parte de la Empresa X de ideas no solicitadas X no obliga a la compañía a mantener confidenciales estas ideas ni obliga a la compañía a remunerar a la persona que las presenta".

Comentario: Esta política establece las expectativas de terceros cuando envían ideas no solicitadas a la Empresa X. El mecanismo típico para recibir tales ideas es a través del correo electrónico, pero las ideas también se pueden recibir a través de otros mecanismos. Si bien el alcance de la política se puede ampliar con el fin de incluir otros mecanismos de comunicaciones además de las páginas en la red de Internet, generalmente sólo las páginas en la red permiten que un aviso se exhiba de manera visible. Por ejemplo, sería difícil pedir que el personal diga estas palabras cuando la gente utiliza el teléfono para entrar en contacto con la organización. Algunas organizaciones pueden ir un paso más allá, especificando que las ideas que se suministran desde el exterior se concentren a través de un contacto interno que no se encuentre en el lado operacional del negocio. Si este contacto estuviera del lado operacional del negocio, podría estar tentado a utilizar la idea para mejorar las operaciones. Esta persona contacto puede entonces hacer seguimiento con el promotor de la idea y pedirle que firme una nota de liberación. Si el promotor rechaza firmar, la persona contacto debe destruir todas las copias a excepción de una copia archivada en sobre sellado y fechado, que se pueda utilizar como evidencia. Este proceso permite que la persona asignada como

promotor diga que fue el único, además del receptor inicial dentro de la Empresa X, que estaba al tanto de la sugerencia. El escrito de esta política podría ampliarse para que incluya las palabras que indiquen que todo el material recibido se convierte en propiedad de la Empresa X.

Políticas Relacionadas:“[Acuerdos de Confidencialidad de Terceros](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

37. Información de Internet en Sistemas de Producción

Política: A excepción de la información proporcionada por clientes potenciales, clientes, proveedores, socios del negocio o agencias gubernamentales, los sistemas informáticos de la Empresa X no deben depender de la información gratuita obtenida a través de Internet.

Comentario: Esta política garantiza que los sistemas informáticos de producción serán sólidos, fidedignos y confiables. No se aconseja confiar en la información gratuita proporcionada por terceros, porque éstos pueden cambiar o retirar tal información a discreción y la organización dependiente después no tendrá ninguna influencia sobre estos cambios o retiros. La política no prohíbe el uso de la información obtenida de Internet si hay un pago de por medio. Sería aceptable, entonces, que una compañía confie en la información provista vía Internet proveniente de una organización de estudios de mercado vía suscripción. Algunas organizaciones pueden suprimir las palabras "agencias gubernamentales" de la política si no consideran esta información confiable u oportuna. Estas palabras fueron incluidas sobre todo para la industria financiera, que obtiene información sobre tasas de interés y otros datos macroeconómicos a través de Internet. Otras organizaciones pueden modificar la política de modo que no se confie únicamente en la información gratuita disponible en Internet. El confiar, en este caso, sería aceptable si la información pudiera ser corroborada de manera independiente.

Políticas Relacionadas:“[Confidabilidad de la Información de Internet](#)” y “[Exploración de Software Descargado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

38. Páginas Web No Oficiales

Política: El patrocinante de cualquier página no oficial en la red que trate sobre los productos o sobre los servicios de la Empresa X debe haber firmado un contrato con el director de Relaciones Públicas.

Comentario: Las organizaciones que no monitorean cuidadosamente y vigilan estas páginas web no oficiales pueden verse en apuros legales que incluyen tergiversación, infracción de marca registrada y violación del derecho de autor. La finalidad de esta política es tomar una posición enérgica contra tales páginas no oficiales en la red, a menos que el operador se comprometa en términos aceptables con el director de Relaciones Públicas. Uno de estas cláusulas debe ser que la Empresa X puede, en cualquier momento y por cualquier razón, exigir al operador que retire alguna o todas las referencias a sus productos y a los servicios de la Empresa X. Se recomienda que la palabra "no oficial" aparezca en estas páginas en la red, junto a otras palabras que demuestran claramente que la Empresa X no patrocina o no se hace responsable por la página. Algunas organizaciones pueden considerar tales páginas no oficiales en la red como buena publicidad. No obstante, de permitirse tales páginas caseras no oficiales, la organización afectada debe ejercer sobre éstas un control estricto a través de un contrato legal. Se recomiendan las discusiones con el consejero legal interno, porque pueden perderse ciertos derechos legales si éstos no se reafirman. Por ejemplo, si una organización permite que otras utilicen su marca registrada sin su autorización, arriesga la pérdida de sus derechos. Esta política prohíbe al personal propio construir páginas web sin el previo consentimiento por escrito del director de Relaciones Públicas.

Políticas Relacionadas: "Excepción de Responsabilidad en Mensajes Personales en Internet" y "Sistemas Web Con Nombres Similares"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

39. Páginas Web Personales

Política: Todo trabajador que use los sistemas proporcionados por la Empresa X debe firmar una declaración donde reconoce que es responsable de todo el contenido que publique en ese sitio, antes de que su sitio web entre en funcionamiento, y que la Empresa X se reserva el derecho de revocar el acceso a cualquier persona en cualquier momento.

Comentario: Esta política otorga a los trabajadores un mecanismo libre para crear y para publicar sus propias páginas personales en la red. Un mayor número de organizaciones ahora ofrece esa posibilidad. Los usuarios publican gráficos o preparan un resumen de su experiencia y responsabilidades actuales en la Empresa X. Esta política define quién tiene la responsabilidad de la página, aunque la Empresa X haya proporcionado los computadores y otras instalaciones de apoyo. Un peligro de las páginas personales accesibles por Internet es que las agencias de empleo pueden fácilmente identificar y emplear personal con talento técnico superior, puesto que su información personal es de fácil acceso. La ventaja de adoptar el mecanismo descrito en esta política, es que la Empresa X puede fácilmente determinar lo que están publicando sus trabajadores en Internet, tener cierto control sobre el contenido y poder revocar su acceso si no está de acuerdo con el mismo.

Políticas Relacionadas: "Excepción de Responsabilidad en Mensajes Personales en Internet" y "Páginas Web No Oficiales"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

40. Comisión Administradora de Página Web de Internet

Política: Previo a su publicación, todos los cambios a la página web corporativa de Internet de la Empresa X deben ser aprobados por una comisión especial establecida por el departamento de Relaciones Públicas que garantice que todo el material publicado tenga un aspecto consistente y bien acabado, esté alineado con las metas de negocio y esté protegido por medidas de seguridad adecuadas.

Comentario: Esta política refleja una solución práctica donde las decisiones sobre el material fijado a un sitio web se delegan a una comisión administradora. Estas decisiones pueden también requerir una autorización de la alta gerencia. La comisión incluye típicamente a algunos administradores de sistema en la red, un especialista en seguridad de la información, un abogado especialista en propiedad intelectual, un experto en comercialización y un experto en relaciones públicas. Esta política sería distribuida ordinariamente sólo al personal técnico de los sistemas informáticos porque típicamente sólo ellos tienen los privilegios de acceso para realizar cambios.

Políticas Relacionadas: "Aprobación de las Representaciones Públicas" y "Remoción de Material Ofensivo"

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

41. Diseño de Página Web en Internet

Política: Todas las páginas en Internet de la Empresa X se deben elaborar conforme a las normas de diseño, normas de navegación, las frases legales normalizadas y demás requisitos similares especificados por la Comisión Administradora de Páginas Web en Internet.

Comentario:Esta política aclara que todas las páginas en Internet deben elaborarse conforme a un sistema normalizado de requisitos. Más que describir explícitamente los requisitos en la política, ésta solamente indica que existen y que todas las páginas en la red deben elaborarse de conformidad con dichos requisitos. Esto se hace de esta manera porque los requisitos pueden cambiar. Los artículos típicos a incluir en la lista de los requisitos son:

- "Aclarar las transferencias de la sesión de un usuario del sitio web de la Empresa X a la página web de otra organización.
- "Aclarar las transferencias de Internet a la intranet .
- "Colocar el nombre de la Empresa X en todas las páginas para evitar que otros sitios se vinculen a estas páginas y digan de manera indirecta que el material es propio.
- "Incluir una renuncia en las páginas vinculadas que indique que la Empresa X no es responsable del material encontrado en los sitios referidos.

Políticas Relacionadas:["Aprobación de las Representaciones Públicas"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

42. Establecimiento de Enlaces Calientes en Internet

Política: Todos los vínculos que transfieran la sesión de Internet de un usuario de un sitio web de la Empresa X a un sitio web de cualquier ente externo, deben estar autorizados por la comisión administradora de la página web de Internet.

Comentario:Esta política evita que los diseñadores y los administradores del sitio web y otros sitios internos de manejo en la red, establezcan vínculos con otros

sitios que pueden desacreditar a la Empresa X. Puesto que cada vínculo implica el endoso de la Empresa X, todas las propuestas de vínculos deben ser revisadas por una comisión o previamente autorizadas por el ejecutivo a cargo. En algunos casos se deben establecer criterios específicos y los entes externos deben satisfacer estos criterios antes de establecer cualquier vínculo. Los criterios pueden incluir una brillante reputación del ente, no estar en competencia directa con la Empresa X, ser de interés a los que visitan el sitio web de la Empresa X y la voluntad de establecer dicho vínculo de modo recíproco.

Políticas Relacionadas:["Guía de Estilo de Intranet"](#) y ["Excepción de Responsabilidad en Enlaces Calientes Hacia Internet"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

43. Excepción de Responsabilidad en Enlaces Calientes Hacia Internet

Política: Todos los vínculos que transfieran desde un sitio web de la Empresa X que visualiza un usuario conectado a Internet, a un sitio web asociado a un tercero, deben estar acompañados por una declaración de excepción de responsabilidad claramente exhibida previamente aprobada por el departamento jurídico.

Comentario:Esta política evita que los clientes, los clientes potenciales y otros aleguen que la Empresa X es responsable legalmente por el comportamiento del personal del tercero, de sus productos o de sus servicios. Una persona que crea estar agraviada demandará a todos aquellos asociados, con la intención de obtener dinero o algún otro tipo de beneficio. Una persona agraviada puede alegar que la existencia de un vínculo del sitio de la Empresa X a un tercero, se entendía como un endoso de sus productos o sus servicios. Esta política requiere una declaración de excepción de responsabilidad que expresamente rechace todos los supuestos endosos implícitos. La redacción de la declaración cambiará en el tiempo tal como evolucione la ley en Internet y, por esta razón, los detalles de la redacción de la declaración no están incluidos en la política.

Políticas Relacionadas:["Comisión Administradora de Página Web de Internet"](#) y ["Establecimiento de Enlaces Calientes en Internet"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

44. Revisión de Página Web en Internet

Política: Un integrante del personal del departamento de Mercadeo debe revisar diariamente la página web de la Empresa X para confirmar que la página está funcionando, que no se ha realizado ningún cambio no autorizado y que no se han establecido vínculos no autorizados.

Comentario: Esta política detecta una modificación en la página web de la Empresa X. Los hackers cambian a menudo las páginas en la red para promover una causa o para desacreditar la organización que publicó el material. Pueden también agregar vínculos a sitios que probablemente desacrediten a la organización. Esta política garantiza que las páginas web modificadas o los vínculos no serán permanentes y que serán cambiados con prontitud. Los clientes a menudo elevan este tipo de ataques a la atención de la organización. Pero, en el caso que los clientes u otros terceros no hayan reportado tales cambios, esta política hace que un integrante del personal lo haga al revisar la página web. La política es un mecanismo para aquellas organizaciones que no desean invertir en un sistema de detección de intrusiones. Para otras organizaciones que tengan suficientes fondos disponibles, una mejor opción es el empleo de un paquete de software que detecte automáticamente cambios a una página web y notifique al personal técnico o directamente al sistema de administración en la red.

Políticas Relacionadas: “Modificación de la Información de Negocio de Producción” y “Desactivación, Cambio o Eliminación de Registros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

45. Cambios en Contenido de Sitio Web en Internet

Política: Todos los sitios en la red de la Empresa X deben estar diseñados y puestos en servicio de manera que cada cambio no autorizado al contenido del sitio sea detectado y corregido inmediata y automáticamente.

Comentario: Esta política requiere que el personal técnico de la Empresa X utilice una variedad de productos para detectar inmediatamente cambios no autorizados en los archivos del contenido del sitio web, para después restablecer automáticamente el contenido autorizado. Aunque esta funcionalidad no es común, no es difícil de programar mediante firmas digitales. Ciertos productos se pueden utilizar para detectar

cambios inmediatamente, seguidos por la ejecución de un programa que recargue el contenido autorizado de un CD-ROM u otro tipo de medio de almacenamiento de datos de sólo lectura. Esta política trata una de las áreas más difíciles en la gestión de páginas web. Los hackers y los activistas políticos han obtenido en varias ocasiones acceso no autorizado a páginas en la red, para después cambiar el contenido y desacreditar a la organización patrocinante de dicha página.

Políticas Relacionadas: “Comisión Administradora de Página Web de Internet” y “Archivos de Sitios Web y Comerciales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

46. Ataques a Páginas Web

Política: Antes de poner en servicio un servidor de páginas web que había sido deteriorado, todas las páginas en la red, el software del sistema y los archivos de la configuración de sistema deben ser verificados para identificar cambios.

Comentario: Esta política evita que los administradores del servidor de páginas web restaren una página web a su estado original, colocando en línea el servidor de páginas web en Internet inmediatamente después de un ataque dañino. El problema puede ser mucho más profundo y los hackers pueden haber tomado control del servidor. Es por esta razón que se deben revisar todos los archivos del software del sistema y de la configuración. Esta revisión no tiene sentido si se hace manualmente, no sólo porque tiende a errores, sino por el gran consumo de tiempo.

Políticas Relacionadas: “Cambios en Contenido de Sitio Web en Internet” y “Revisión de Página Web en Internet”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

47. Almacenamiento de Información Financiera de Clientes

Política: La Empresa X no debe almacenar ninguna información financiera del cliente en sus servidores de la red, en los servidores del comercio de Internet, en los servidores de la base de datos de Internet o en otros sistemas que estén conectados directamente a Internet.

Comentario: Esta política evita que la información financiera del cliente sea visualizada por hackers u otros terceros no autorizados. La intención de la política es remover toda la información financiera de los servidores en la red y otros sistemas directamente accesibles a través de Internet y colocarla bajo la protección de varios sistemas cortafuegos. Este tipo de información se puede registrar y almacenar, pero no en sistemas que estén conectados a Internet. Una alternativa a esta política sería el cifrado de dicha información financiera.

Políticas Relacionadas: “[Divulgación de Información Financiera](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

48. Nombre de Dominio en Internet

Política: El nombre del dominio en Internet de la Empresa X se debe registrar sólo con una empresa que proporcione procedimientos apropiados de seguridad y de control de cambios.

Comentario: Mediante esta política se garantiza que ningún tercero no autorizado cambiará la información de registro de Internet referente al nombre del dominio de la Empresa X. Esto puede suceder si una organización utiliza mecanismos poco seguros en la autenticación del usuario para realizar cambios. Hay métodos más seguros para autenticar la identidad de una persona que inicia un cambio en un nombre del dominio, lo que incluye solicitar el cambio vía papel con membrete, contraseñas cifradas y firmas digitales.

Políticas Relacionadas: “[Registros de Nombres de Dominio en Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

49. Respuestas a Comandos en Servidores Internet

Política: Los servidores de Internet deben ser modificados de manera que las respuestas prolíjas proporcionadas a ciertos comandos no revelen la información del software instalado en el servidor.

Comentario: Esta política garantiza que la organización no revelará información de manera involuntaria respecto de sus sistemas o software. Los vendedores del software

del servidor envían a menudo su software con defectos que proporcionan respuestas prolíjas a ciertos comandos. Esto les permite determinar cuáles organizaciones utilizan su software. Estas respuestas pueden revelar información que puede ayudar significativamente a los intrusos. Una respuesta abreviada es en la mayoría de los casos equivalente a una respuesta prolíja.

Políticas Relacionadas: “[Establecimiento de Enlaces Calientes en Internet](#)” y “[Compartir Información de Mercadeo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

50. HTML del Sitio Web

Política: Todo código de hipertexto usado en sitios web de la Empresa X deben ser revisados con un programa depurador o rutina de eliminación de información confidencial, antes de ser colocado en servicio en cualquier servidor conectado a Internet para actividades de producción.

Comentario: Esta política supera una de las características del lenguaje de hipertexto (HTML, por sus inglés en inglés), que permite que cualquier curioso lea no solamente el código mismo, sino también todos los comentarios insertos. La política dice que los programadores de HTML o el responsable del sitio web deben quitar los comentarios, nombre del proyecto, nombre del desarrollador y otra información que puede ser usada por los hackers, espías industriales, ex-empleados descontentos y otros. Tal información puede ser usada para adivinar la contraseña o quizás en un ataque al sitio. Procesar el código HTML a través de un depurador también lo optimiza, dando como resultado una ejecución más rápida. La política se puede ampliar para incluir un depurador o un ofuscador para JavaScript, que hacen que dichos programas se ejecuten más rápidamente porque eliminan comentarios y espacios en blanco. Un depurador u ofuscador de JavaScript hace además la ingeniería inversa más costosa y lenta.

Políticas Relacionadas: “[Mensaje de Advertencia en Inicio de Sesión](#)” y “[Respuesta por Inicio Incorrecto de Sesión](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

51. Información Secreta en la Web

Política: La información secreta de la Empresa X no debe estar almacenada en los servidores Internet o de la intranet.

Comentario: Esta política reconoce que se toman riesgos adicionales al usar tecnología Internet o intranet. Para prevenir el acceso no autorizado al tipo de información más sensible, ésta se debe manejar por medios más tradicionales, incluyendo reuniones y llamadas telefónicas personales. El tipo más sensible de información en esta política ha sido identificada como secreta, pero la identificación puede cambiar de acuerdo al sistema de clasificación interno de datos en uso.

Políticas Relacionadas: “Aislamiento de Sistemas con Información Secreta”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

52. Información Secreta en Intranet

Política: El acceso a las aplicaciones en la intranet que manejan la información secreta sólo se debe permitir cuando se emplee una red privada virtual.

Comentario: Esta política garantiza que los datos secretos que viajan en una intranet no serán interceptados por terceros no autorizados que pudieran haber instalado equipos de espionaje. Preocuparse por dichos equipos es razonable, porque la mayoría de los incidentes de seguridad ocurren por el personal interno, quienes en muchos casos tienen el conocimiento, la habilidad y el acceso para causar graves daños. Una red privada virtual (VPN, por sus siglas en inglés) evitará la intercepción en la intranet porque cifra todas las transmisiones. Muchas VPN también proporcionan autenticación extendida del usuario, más allá del mero identificador de usuario y contraseña fija que puede requerir el computador de destino. Este nivel adicional de autenticación de usuario puede ayudar aún más a restringir el acceso a la información secreta.

Políticas Relacionadas: “Conexiones en Red con Organizaciones Externas” y “Modem por Cable”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

53. Información de Contacto en Seguridad

Política: Todas las páginas de apertura de todos los sitios Web de la Empresa X deben incluir información de contacto para el departamento de Seguridad Informática.

Comentario: Esta política garantiza que los externos que identifiquen un problema, podrán reportar rápidamente sus observaciones a la persona correcta. La política pide a los externos apoyar la seguridad informática. A menudo, los clientes y los posibles clientes son los primeros en darse cuenta de que existe un problema, aunque los sistemas de detección de intrusiones son los que tienen que notificar al personal pertinente. La inclusión de tal información de contacto en las páginas web también permite a los externos reportar problemas que no son de seguridad, tales como el tiempo lento de respuesta o los resultados fallidos de un cálculo. Algunas palabras que pueden acompañar a la información de contacto podrían ser, “Por favor, reporte cualquier sospecha de violación de seguridad o problemas a”. El alcance de esta política podría ampliarse a todos los sitios de la intranet.

Políticas Relacionadas: “Reportes Externos de Violaciones” e “Informes de Incidentes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

54. Investigación Pública

Política: Cada vez que la Empresa X lleve a cabo encuestas, estudios analíticos u otra investigación destinada al consumo público, los participantes de esta investigación deben mencionar en su reporte tanto al patrocinante como todos los conflictos de intereses potenciales.

Comentario: Esta política restaura la integridad de la recopilación de noticias, investigación sobre drogas, investigación de mercado y tópicos asociados que han sido perjudicados por denuncias relacionadas con conflicto de intereses. Si un investigador, tal vez un profesor universitario, estuviese asesorando, como trabajo adicional, a una empresa farmacéutica para evaluar una nueva droga, este hecho debería divulgarse. El hecho de que una empresa farmacéutica le esté pagando a un profesor para que evalúe una droga debe divulgarse en los descubrimientos publicados. El no revelar dicha información se puede considerar capcioso. Si bien el uso de esta política en varias organizaciones puede requerir una reformulación o un ajuste, la idea es fundamentalmente útil, con el objetivo de promover un

clima de negocios caracterizado por la integridad y el juego limpio. Un posible ajuste en las palabras incluye la divulgación de cualquier restricción sobre los resultados de la investigación especificados antes de iniciar el proyecto. Esta política sólo es importante si la Empresa X publica boletines informativos, reportes de investigación o material similar.

8.07.07 Otras formas de Intercambio de Información

1. Grabación de Comunicaciones en Internet

Política: Los usuarios finales no deben grabar ninguna de sus interacciones con grupos a larga distancia a través de Internet, a menos que dichos grupos a larga distancia estén al tanto de que las transmisiones están siendo grabadas.

Comentario: Esta política evita una ruptura en las relaciones de confianza, así como las acusaciones de violación a la privacidad y la mala publicidad. Mucha gente se sorprenderá al saber que las charlas retransmitidas a través de Internet y los mensajes de interacción instantáneos puedan ser grabados fácilmente. En una forma indirecta, esta política advierte a los usuarios internos que terceros pueden grabar sus interacciones. Uno de los mayores peligros asociados con estos servicios es que se utilizan generalmente para transmitir mensajes muy informales que se espera desaparezcan cuando termine la interacción. Los participantes pueden rápidamente hacer comentarios engorrosos o hasta calumniar a terceros. Ambos servicios han añadido recientemente una característica de archivo, lo cual hace que estas interacciones sean potencialmente tan permanentes como los correos electrónicos archivados. La política no menciona nada sobre los registros realizados por la organización que suministra los computadores y las redes de trabajo. La política sólo se relaciona con usuarios finales.

Políticas Relacionadas: “Recopilación Furtiva de Información Privada” y “Uso de Tecnología Telefónica para Conferencias o Grabación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Divulgación Telefónica de Información

Política: La información solicitada sobre el cliente no debe ser revelada telefónicamente, a menos que la persona que llama sea capaz de identificarse a través de

Políticas Relacionadas: “Segundos Trabajos” y “Acuerdos de Confidencialidad con Antiguos Patronos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

un código secreto compartido o a través de otras medidas de identificación de las personas que efectúan las llamadas, con autorización de la gerencia de la Empresa X.

Comentario: Esta política evita que los trabajadores internos divulguen inadecuadamente información personal o privada, si la persona que llama no se ha identificado adecuadamente. Esta política también evita que el personal del Centro de Atención al Usuario sea engañado por hackers utilizando técnicas de ingeniería social. Mientras los especialistas de mercadeo pueden considerar esta política como una barrera para llevar a cabo negocios rápida y eficientemente, dicha política es necesaria si una organización divulga alguna información telefónicamente. Esta política puede ofrecer a los clientes seguridad adicional de que su dinero y su información están protegidos adecuadamente. El mismo enfoque podría ser utilizado para las transacciones telefónicas. Si la política incluyera transacciones, un integrante del personal de la compañía telefónica podría negarse a reenviar llamadas de un número telefónico del negocio, basado simplemente en un requerimiento hecho vía telefónica. En vez de esto, devolvería la llamada al cliente a un número conocido o de alguna otra manera trataría de establecer una identificación positiva.

Políticas Relacionadas: “Ordenes para Cambiar Registros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

3. Discusiones En Sitios Públicos

Política: Todos los trabajadores deben evitar discutir información privada de los clientes en lugares públicos, tales como los vestíbulos de los edificios o en los transportes públicos, a menos que se haya obtenido un permiso explícito por parte del cliente.

Comentario: Muchas organizaciones tales como los hospitales dependen de manera crítica del hecho de que los clientes revelen información privada. Si los clientes se guardan esta información privada, porque les preocupa que entes no autorizados puedan acceder a ella, entonces la calidad del producto o del servicio que suministra la organización estará comprometida en gran medida. Si a un paciente le preocupa que su doctor discuta su caso en un pasillo frente a otros pacientes, dicho paciente puede no mencionar el tipo de medicamento que está tomando. Esto puede llevar a una situación peligrosa donde nuevas drogas prescritas interactúen con medicación secreta y causen reacciones serias que pudieron haber sido evitadas. Esta política enfatiza la importancia de mantener la información privada en sitios restringidos, tales como un consultorio médico. La política prohíbe toda discusión en lugares públicos. Sin importar si la identidad del cliente está oculta, esta posición es necesaria porque los trabajadores pueden no estar atentos y divulgar información a través de la cual se pueda descubrir la identidad del cliente. Nada de lo incluido en esta política evita que los trabajadores hablen acerca de los resultados de sus investigaciones en un sentido general, tal vez incluyan conclusiones estadísticas, pero evitando mencionar casos específicos. Si existe la necesidad de hablar de casos específicos, como por ejemplo una presentación en una conferencia, se puede obtener un permiso por adelantado de los individuos.

Políticas Relacionadas: “[Información Estadística de los Registros de los Clientes](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Clientes Rechazan Correo Directo No Solicitado

Política: Los clientes de la Empresa X deben recibir la oportunidad de informar a la Empresa X que no desean ser contactados a través de promociones no solicitadas de promociones vía correo directo.

Comentario: Esta política le permite al cliente decir a la Empresa X que no desea recibir correo masivo sobre promociones. Se debe notificar al cliente que puede contactar a la Empresa si no desea recibir solicitudes a través del correo. Esta notificación puede insertarse o imprimirse dentro de los estados de cuenta. La política le prohíbe a la Empresa X vender estos detalles de contactos de los clientes a terceros, los cuales pueden utilizarlo para correo masivo. Si un cliente solicita información a través del correo, aun cuando dicho

cliente haya expresado previamente su deseo de no recibir correo directo, esta política permitirá que se le envíe la información. La política podría expandirse para incluir solicitudes de fax, solicitudes de telemarcadeo y solicitudes de correo electrónico, particularmente porque el uso de estos sistemas de comunicación se está incrementando para el envío del equivalente a correo basura. Si su alcance se expande, esta política evitará que se violen varias leyes y reglamentos.

Políticas Relacionadas: “[Registros de Telemarcadeo](#)” y “[Opción de Participación en Sistema de Datos Privados](#)”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

5. Divulgación de Información Financiera

Política: Toda revelación de información relativa a la situación financiera de la Empresa X, a los cambios anticipados en la posición financiera y a los desarrollos de los negocios, de la cual se pudiera esperar una modificación sustancial de la impresión que los inversionistas tienen de la empresa, debe ser autorizada con anterioridad por el departamento de Relaciones Públicas o un vicepresidente y debe hacerse disponible públicamente para todos los inversionistas y partes interesadas al mismo tiempo.

Comentario: Esta política evita que cualquier trabajador haga revelaciones seleccionadas a ciertos analistas de seguridad, los cuales utilizan esta información para formular compras, ventas o dar recomendaciones referentes a las acciones de la Empresa X. Este enfoque tradicional permite que la gente que cuenta con el conocimiento de esta información confidencial pueda beneficiarse en la bolsa de valores, mientras que el público general no puede. Desde el punto de vista de la seguridad informática, hay que tener mucho cuidado en cuanto a las divulgaciones al público, especialmente en un ambiente de negocios litigantes. Esta política nos lleva a desarrollar una mayor conciencia y un mayor interés en cuanto a lo que se divulgue públicamente y a un mínimo de imparcialidad en el proceso de divulgación. Esta política sólo es pertinente para las empresas que se encuentran en la lista de la bolsa de valores.

Políticas Relacionadas: “[Transferencia de Información a Terceros](#)” y “[Registros de Divulgación de Información Privada — Detalles](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad:Todos

6. Envío de Información Secreta

Política: La información secreta debe ser enviada a través de correos internos o externos en sobres opacos y sellados que digan: "Para ser abierto sólo por el destinatario," dentro de otro sobre que no especifique la sensibilidad del contenido.

Comentario: Esta política gira a todos los trabajadores de la Empresa X instrucciones específicas en cuanto a la manera correcta de señalizar la información secreta a ser enviada a través de las diferentes vías de correo. La política está dirigida al tipo de información más sensible, pero no se aplica a la información de menos sensibilidad. La información privada y confidencial se puede manejar por medio de otra política. Un sobre opaco evita que personas no autorizadas tomen el sobre y lo lleven hacia un lugar iluminado para leer el contenido. El sobre externo se utiliza para no llamar la atención de aquellas personas que estén buscando tal información. Las palabras: "Para ser abierto sólo por el destinatario" son también una medida para no llamar la atención y para especificar sutilmente que el contenido puede ser sensible. Algunas organizaciones quisieran eliminar esta parte de la política. No hay evidencia en ninguno de los dos sobres acerca de la sensibilidad del contenido. El uso de la palabra "sellado" es para indicar que los sobres reutilizables no son apropiados para este tipo de material. Es importante que el receptor se entere de si alguien no autorizado ha examinado el material durante su tránsito. Esta política asume la asistencia de otra política que define el término "secreto", que puede ser reemplazado fácilmente con la etiqueta utilizada dentro de la organización.

Políticas Relacionadas:“Presentación de la Imagen Pública,” “Envío de Información Privada y Confidencial,” “Clasificación de Datos en Cuatro Categorías,” y “Envío de Información Sensible”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

7. Envío de Información Sensible

Política: Si la información privada, confidencial o secreta se envía a través de correo interno, correo externo o vía servicio de mensajería, debe estar dentro de dos sobres o contenedores, donde el sobre o contenedor externo no especifique la sensibilidad de la

información allí contenida y el sobre o contenedor interno, sellado y opaco esté etiquetado "Privado," "Confidencial," o "Secreto".

Comentario: Esta política gira a todos los trabajadores de la Empresa X instrucciones específicas en cuanto a la forma más apropiada de señalizar la información privada, confidencial o secreta enviada a través de varios tipos de correo. La política puede ser utilizada para todo tipo de información sensible, en vez de tener políticas diferentes para diferentes clasificaciones de información sensible. Un sobre opaco evita que las personas no autorizadas lleven el sobre a un lugar iluminado y lean el contenido del mismo. El sobre externo evita llamar la atención de aquellos que buscan este tipo de información. Esta política asume la existencia de una política que define los términos "privada, confidencial o secreta".

Políticas Relacionadas:“Presentación de la Imagen Pública,” “Clasificación de Datos en Cuatro Categorías” y “Envío de Información Secreta”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

8. Transmisión de Información Secreta en Papel

Política: La información secreta en copias impresas en papel debe ser enviada a través de un servicio confiable de mensajería o de correo certificado.

Comentario: Esta política informa a los trabajadores que deben utilizar los métodos de transporte más seguros para enviar información secreta impresa. Un transporte especial y confiable constituye una garantía para la información de mayor sensibilidad. La política no está dirigida a la información guardada en los medios de almacenamiento de datos informáticos ya que ésta debe estar cifrada y puede ser enviada por cualquier medio, sin temor alguno de que sea divulgada sin autorización. Esta política no abarca los contenedores utilizados para la información secreta en copias impresas. Esta política asume la existencia de una política que define el término "secreta".

Políticas Relacionadas:“Envío de Información Sensible” y “Clasificación de Datos en Cuatro Categorías”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

9. Firmas Legales

Política: Todas las firmas de contratos, de órdenes de compra y de otros documentos legalmente vinculantes suministrados por terceros deben estar en papel.

Comentario: La política garantiza que la Empresa X estará capacitada para suministrar la evidencia adecuada de la existencia de acuerdos legalmente vinculantes, tales como órdenes de compra. Si dichos acuerdos están plasmados en papel fax, algunos jueces pueden alegar que ésta no constituye una evidencia suficiente. Nada de lo incluido en esta política impide que los trabajadores posean un fax con firmas como documento preliminar, a ser seguidas después por las firmas en papel tradicional. Este enfoque de dos fases permite que se ponga en marcha el trabajo inmediatamente, ya que los documentos sólo constituyen una formalidad legal. Esta política es también importante para el correo electrónico y otras formas de comunicación del negocio. Algunas jurisdicciones reconocen cada vez más las firmas digitales y los certificados digitales como legalmente vinculantes.

Políticas Relacionadas: “[Contratos en Línea con Intercambio de Papel y Firmas](#)” y “[Contratos Obligatorios en Sistemas Electrónicos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Conversaciones Telefónicas Sobre Información Sensible

Política: Los trabajadores deben evitar discutir información sensible a través del teléfono.

Comentario: Esta política informa a los empleados que los teléfonos pueden estar intervenidos o interceptados y les pide no discutir información sensible cuando los utilicen. En este contexto, se pueden mencionar trucos como el uso de palabras codificadas o sobrenombres. La política podría extenderse para incluir las instalaciones para videoconferencias, las cuales a menudo no están cifradas y, por lo tanto, pueden ser interceptadas. Esta política asume que la organización ya ha definido el término "sensible" en una política.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

11. Teléfonos Celulares o Inalámbricos

Política: La información secreta de la Empresa X no se debe discutir nunca en teléfonos inalámbricos o celulares no protegidos con cifrado.

Comentario: Esta política evita la divulgación de la información sensible. Un gran número de casos muy publicitados dejan claro que es fácil y económico interceptar las conversaciones que se envían a través de las ondas hertzianas. Ésta es una política especialmente importante para la alta gerencia, que generalmente posee tales teléfonos, a menudo no entiende la tecnología asociada y generalmente discute asuntos secretos. El alcance de esta política puede expandirse e incorporar otras redes inalámbricas, tales como servicios de comunicaciones personales, asistentes personales digitales con capacidades inalámbricas, buscaperonas alfanuméricos, redes de área local inalámbricas, sistemas de radio móvil especializados, redes de radioaficionados, redes de paquetes inalámbricos y redes satelitales.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” e “[Información Sensible en Máquinas Contestadoras](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

12. Transmisión Inalámbrica de Información Secreta

Política: No se debe utilizar tecnología inalámbrica para la transmisión de información secreta no cifrada.

Comentario: Interceptar las transmisiones de radio es bastante fácil y se pueden obtener muchos detalles útiles tales como números telefónicos, identificadores de usuarios y contraseñas. Esta política informa a los usuarios que no deben utilizar tecnología inalámbrica, a menos que sepan que las transmisiones están cifradas. Desafortunadamente, no está disponible el cifrado para varios de estos sistemas, tales como los micrófonos "lavalier" especializados utilizados por los locutores, así que prohibir el uso de estos sistemas para la información secreta es la única opción. Esta política asume que la palabra "secreta" ha sido claramente definida en alguna otra parte.

Políticas Relacionadas: “[Protección Contra la Radiación Electromagnética](#)” y “[Teléfonos Celulares o Inalámbricos](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

13. Exposición Pública de Información Sensible

Política: La información secreta, confidencial o privada de la Empresa X no se debe leer, discutir o exponer en los aeropuertos, los restaurantes, los ascensores, los transportes públicos u otros sitios públicos.

Comentario: Esta política evita la divulgación no autorizada de la información sensible. No es inusual que los empleados trabajen mientras van en un autobús, un avión u otro transporte público y a menudo lo hacen con información sensible. La política evitará que otros viajeros miren por encima del hombro en el avión, lean el material mientras utilizan la misma mesa en un restaurante o de alguna manera estén expuestos al material. La política no abarca aquellas circunstancias donde la información se haya perdido o haya sido robada. La palabra "sensible" se puede utilizar en vez de "secreta, confidencial o privada." La política asume que ha sido emitida una política de clasificación de datos que explica estos términos.

Políticas Relacionadas: "Viajes con Información Secreta," "Clasificación de Datos en Cuatro Categorías," y "Posiciones de las Pantallas de los Computadores"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

14. Discusiones En Areas Administrativas

Política: Los trabajadores de la Empresa X no deben discutir información secreta en áreas administrativas que incluyan, sin limitantes, corredores, cafeterías, áreas de recepción de visitantes y lavabos, debido a que en estas áreas puede haber personas que no están autorizadas para recibir dicha información.

Comentario: Esta política define dónde se puede discutir información secreta dentro de las instalaciones de la Empresa X. Los trabajadores pueden pensar que una vez que se encuentran en las instalaciones de la Empresa X, pueden discutir sobre cualquier tema, no importa cuán sensible sea la información. La política hace énfasis en cuanto a la diferencia entre aquellas personas que están autorizadas a recibir la información secreta y aquellas que no lo están. La política se debe utilizar conjuntamente con un sistema de clasificación

de datos, el cual se puede utilizar para restringir el acceso de los trabajadores a la información por medio de una etiqueta.

Políticas Relacionadas: "Exposición Pública de Información Sensible," "Discusiones En Sitios Públicos," y "Teléfonos Celulares o Inalámbricos"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Alto

15. Asistentes a Reuniones

Política: Las personas que no aparezcan como invitadas o con una autorización previa por parte de la gerencia no deben asistir a las reuniones donde se discutirá información secreta.

Comentario: Esta política gira instrucciones a los trabajadores en el sentido de que aquellas personas que no hayan sido invitadas no asistan a las reuniones donde se discute información secreta. Permitir esta asistencia alteraría al grupo de personas que han sido autorizadas para acceder a la información. Esta política se aplica a las reuniones en vivo, a las teleconferencias y a las reuniones virtuales, donde los participantes se conocen unos a otros en línea. El término "secreto" puede ser sustituido por la etiqueta que contiene la clasificación de datos de mayor sensibilidad utilizada por la Empresa X. Esta política asume que el término "secreto" ha sido definido.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" e "Información Confidencial en Reuniones"

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

16. Reuniones con Terceros

Política: Si los trabajadores que se encuentran en las inmediaciones de un salón de conferencias manejan información sensible, todas las reuniones con terceros visitantes en las instalaciones se deben realizar en salones de conferencia totalmente cerrados, si estos terceros no están autorizados a acceder a dicha información sensible.

Comentario: Esta política evita que la información sensible sea expuesta a terceros. Para reducir las posibilidades de que esto ocurra, los salones de conferencias deben estar rodeados de paredes hasta el techo y con una puerta que funcione. Muchas oficinas cuentan con

espacios abiertos y no tienen paredes o puertas adecuadas, dando como resultado que los sonidos de las áreas circunvecinas puedan ser escuchados por los visitantes. Desde el punto de vista de construcción del edificio, los visitantes no deberían tener la necesidad de pasar cerca de las áreas con información sensible, para llegar al salón de conferencias o para ir al baño. Esta es una razón por la cual las salas de conferencias están ubicadas a menudo en un área pública, fuera de los puntos de control de acceso.

Políticas Relacionadas:“Escritorios Limpios — Horas No Hábiles”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

17. Información Confidencial en Reuniones

Política: Si se discute información confidencial verbalmente en una reunión, seminario, conferencia o presentaciones asociadas, el conferencista debe comunicar claramente lo confidencial de la información y recordar a la audiencia de tener discreción a la hora de divulgarla a otros.

Comentario: Esta política garantiza que las personas que escuchan información confidencial en una reunión, la manejarán apropiadamente. A menos que se den los pasos necesarios para recordarle a las personas acerca del manejo adecuado de la información hablada, estas pueden divulgarla accidentalmente a terceros no autorizados. Esta política implica que todos los trabajadores que realicen presentaciones deben especificar si la información que van a suministrar es confidencial o no. La política asume que ya ha sido adoptado un esquema de clasificación de sensibilidad de los datos.

Políticas Relacionadas:“Clasificación de Datos en Cuatro Categorías” e “Información Liberada al Público — Autorización”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Medianos y altos

18. Superficies Borrables

Política: Después de que finalice cada reunión, se deben borrar todas las superficies de los pizarrones, pizarrones blancos y ventanas de los salones de conferencias.

Comentario: Esta política garantiza que cualquier información potencialmente sensible escrita en cualquier superficie borrable no sea divulgada accidentalmente a terceros a quienes no estaba dirigida la información. Los salones de conferencia son generalmente de libre acceso. Cualquiera en el edificio puede entrar en ellos y revisar toda la información que se deje allí. Las cerraduras en las puertas y la presencia de una persona puede, en algunas ocasiones, proteger las superficies borrables ubicadas en oficinas particulares. Esta política es a la vez cortés con los próximos usuarios del salón de conferencias que puedan necesitar los pizarrones.

Políticas Relacionadas:“Borrado de Superficies Borrables” y “Equipos de Grabación de Audio o Video”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

19. Borrado de Superficies Borrables

Política: La información sensible que quede impresa, incluyendo, sin limitantes, en pizarrones, pizarrones blancos y ventanas, se debe borrar definitivamente con agua o algún líquido especial, antes de que los receptores autorizados de esta información abandonen el área.

Comentario: Esta política evita la divulgación accidental de información sensible a terceros no autorizados. Si se deja información sensible escrita en un pizarrón, entonces las personas que utilicen a continuación el área, pueden obtener inmediatamente dicha información. La política no menciona la ubicación de los pizarrones. En algunas organizaciones militares, esta política constituye un procedimiento operativo normalizado, y también puede ser apropiada para las organizaciones comerciales.

Políticas Relacionadas:“Asistentes a Reuniones” y “Superficies Borrables”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

20. Representaciones de la Organización

Política: Todas las representaciones relacionadas con el negocio realizadas por los trabajadores de la Empresa X, inclusive, sin limitantes, las realizadas por medio de publicidad, en negociaciones con los sindicatos, en las etiquetas de los productos y en los informes gubernamentales, deben ser confiables en todo momento.

Comentario: Esta política informa a los trabajadores que está prohibido mentir o tergiversar la verdad. En general, la política está dirigida a apartar a la Empresa X y sus empleados de eventuales problemas. Esta política puede ser importante si existen acusaciones contra la gerencia, de que sistemáticamente incita a los empleados a no interpretar adecuadamente la información. Esta política también puede ser útil en demandas legales que impliquen fraude o propaganda engañosa, así como también ayuda a evitar o a defender a la Empresa X de imputaciones por parte de los empleados, en las que éstos alegan que no se les dijo la verdad durante la entrevista para el empleo. Esta política puede también ser útil para evitar ser el blanco de bromas y de humor sarcástico que puedan causar problemas.

Políticas Relacionadas: “[Información Incompleta u Obsoleta](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

21. Aprobación de las Representaciones Públicas

Política: Todas las representaciones, incluyendo, sin limitantes, los anuncios a través de todos los medios de comunicación, página principal de Internet, foros electrónicos, mensajes de correos de voz, mensajes al exterior, deben ser emitidas o autorizadas por el departamento de Relaciones Públicas.

Comentario: Esta política evita que departamentos diferentes lleven a cabo representaciones públicas de la Empresa X en forma independiente. Uno de los mayores problemas que enfrentan las organizaciones es que los departamentos crean sus propias páginas web sin una revisión o autorización interna. A menos que una política como ésta exista, está latente el peligro de que esos esfuerzos independientes puedan poner en apuros a la organización públicamente, confundir a los clientes o generar hechos no deseados. Esta política establece un solo punto de contacto para interactuar con el público. La tecnología de comunicaciones actual permite que mucha gente pueda ser localizada fácilmente, a bajos costos y rápidamente. Esta disponibilidad debe ser moderada a través de controles, para no generar problemas de manera accidental. En un conglomerado de empresas autónomas, así como en una entidad gubernamental mayor, debería estar involucrado el departamento de Relaciones Públicas de cada sucursal, en vez de un departamento de Relaciones Públicas centralizado.

Políticas Relacionadas: “[Páginas Web No Oficiales](#),” “[Representaciones de la Organización](#),” “[Foros Electrónicos Públicos](#),” y “[Comunicaciones Públicas](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

22. Comunicaciones Potencialmente Ofensivas

Política: Cualesquier de las comunicaciones de la Empresa X, inclusive, sin limitantes, las grabaciones de mensajes telefónicos, mensajes de correo de voz y cartas, que puedan ofender o molestar a ciertos sectores de la posible población receptora, deben presentar una advertencia apropiada en la portada, en la introducción o en algún otro lugar, de tal manera que el receptor pueda optar por no recibir dicha información.

Comentario: Esta política está dirigida a reducir el número de quejas sobre los anuncios publicitarios y las comunicaciones de la Empresa X. También está dirigida a informar a los receptores sobre la naturaleza de la información, dándoles una oportunidad para no proceder legalmente. Las organizaciones que envían correos potencialmente ofensivos o material masivo por correo, pone sus solicitudes dentro de un sobre que claramente indica que el material es ofensivo. El receptor puede abrirlo o descartarlo. Aunque la política se podría aplicar a las comunicaciones internas, está dirigida inicialmente a las comunicaciones externas.

Políticas Relacionadas: “[Aviso en Cubierta de Fax](#)” y “[Cubrir Información Sensible](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

23. Información Sensible en Máquinas Contestadoras

Política: Los trabajadores no deben grabar mensajes que contengan información sensible en máquinas contestadoras telefónicas o en sistemas de correo de voz.

Comentario: El propósito de esta política es notificar a los trabajadores que los que reciben los mensajes de las máquinas contestadoras telefónicas, pueden no estar autorizados a recibir información sensible. Los trabajadores simplemente deben pedir al posible receptor de la información que devuelva la llamada. No sólo el que recibe el mensaje puede ser otra persona que no sea el posible receptor, sino también los hackers pueden

recibir los mensajes de una máquina contestadora telefónica sin tener acceso físico a la misma. Esta política puede expandirse e incluir la prohibición del uso de instalaciones con acceso remoto, que permiten a las personas tomar mensajes desde diferentes ubicaciones. Sin embargo, esto puede resultar aburrido e impopular para la comunidad de usuarios. La política también podría expandirse para incluir la información sensible grabada en buscadoras alfanuméricos.

Políticas Relacionadas: “[Información Secreta en Altavoces Telefónicos](#),” “[Grabación de Información Sensible](#),” “[Llamadas Cobro a Destino y a Terceros](#),” y “[Teléfonos Celulares o Inalámbricos](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

24. Uso de Tarjetas de Crédito

Política: Al utilizar los teléfonos públicos, cada vez que las circunstancias lo permitan, los trabajadores deben deslizar las tarjetas telefónicas o de crédito en vez de utilizar el teclado numérico o la bocina telefónica para retransmitir la información sobre la cuenta.

Comentario: Esta política evita que los números donde se puedan cargar llamadas lleguen a manos no autorizadas, para ser luego utilizados para cargar llamadas fraudulentas. Es cada vez más frecuente que estas personas escuchen, observen o graben a la gente que ingresa su información contable en un tablero de teléfono público. La treta de la cámara de video, es quizás la más fácil, dado que la cinta puede verse nuevamente para verificar los números introducidos. Asimismo, si la información a ser cargada es transmitida a través de la bocina del teléfono, otras personas pueden escuchar la información. La forma más segura de evitar estos y otros abusos similares, es deslizar la tarjeta de crédito a través de los lectores de los teléfonos públicos, aunque algunos teléfonos no tienen lectores. Esta es una razón por la cual se utilizan las palabras "cada vez que las circunstancias lo permitan" en la política. Otra razón es que los trabajadores de la Empresa X pueden no tener teléfono o una tarjeta de crédito con ellos. Sin embargo, el no llevar una tarjeta de crédito telefónica puede reducir las probabilidades de pérdida o robo de la tarjeta. Otra razón para utilizar tarjetas de crédito bancarias es que la responsabilidad del usuario por cargos fraudulentos es limitada y en muchas instancias es exonerado completamente.

Políticas Relacionadas: “[Posiciones de las Pantallas de los Computadores](#)” y “[Distintivos de Acceso Extraviados](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

25. Uso de Tecnología Telefónica para Conferencias o Grabación

Política: Al utilizar el teléfono, los trabajadores no deben usar los altavoces del teléfono, micrófonos, altoparlantes, grabadores o tecnologías similares, a menos que hayan recibido el consentimiento tanto del emisor como del receptor de la llamada.

Comentario: Esta política garantiza que ambas partes están en conocimiento de que otras personas están escuchando o puedan posteriormente escuchar la conversación. Puede que tanto el emisor como el receptor de la llamada hablen de manera diferente cuando sepan que otras personas están escuchando la conversación. Si sólo una de las partes de la conversación, tal vez el emisor, sabe cómo utilizar dicho equipo, puede estar violando estatutos federales o locales sobre interrupciones de línea.

Políticas Relacionadas: “[Información Sobre el Monitoreo del Desempeño](#)” y “[Áreas de Monitoreo Electrónico](#)”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

26. Grabación de Videoconferencias

Política: Las sesiones de videoconferencias de la Empresa X no se deben grabar, a menos que esta grabación tenga la autorización previa del gerente de seguridad informática y todos los participantes de las videoconferencias estén al tanto de la grabación.

Comentario: Esta política evita futuras responsabilidades legales. Si las sesiones de videoconferencias no son grabadas, éstas no se pueden producir como evidencia durante los procedimientos de revelación de pruebas u otros artificios legales. En cierta forma similar a una política para las organizaciones que necesiten la rutina de destrucción de mensajes electrónicos vencidos y obsoletos, esta política evita que la información sensible interna sea utilizada de manera perjudicial y para lo que no fue generada. Esta política también limita la cantidad de información que la organización debe administrar.

Políticas Relacionadas:“[Monitoreo o Grabación de Conversaciones Telefónicas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

9 CONTROL DE ACCESO

9.01 Requisitos para el Control de Acceso

9.01.01 Política de Control de Acceso

1. Actividades del Hacker

Política: Los trabajadores no deben utilizar los sistemas informáticos de la Empresa X para dedicarse a actividades de "hacking" incluyendo, sin limitantes, el acceder en forma no autorizada a cualesquiera otros sistemas informáticos, para dañar, alterar o irrumpir las operaciones de otros sistemas informáticos y capturar o de algún modo obtener las contraseñas, las claves de cifrado u otro mecanismo de control de acceso que permitan un acceso no autorizado.

Comentario: Esta política establece la posición de la gerencia, que prohíbe las actividades de "hacking" a través de los sistemas informáticos de la Empresa X. Esta política es recomendable en aquellas jurisdicciones donde la actividad de "hacking" no es aparentemente ilegal. La política es también necesaria en la universidad, donde dicha actividad de "hacking" se justifica a nombre de llevar a cabo una investigación informática o para la cátedra de Informática. La política está escrita de tal manera que es aplicable a los sistemas informáticos tanto internos como externos. La política abarca una vasta variedad de técnicas de "hacker", incluyendo la ingeniería social y los capturadores de contraseñas. Las palabras "mecanismos para el control de acceso" son deliberadamente vagas. Esto incluiría tarjetas inteligentes, mecanismos de contraseñas dinámicas y otros mecanismos extendidos de autenticación. Esta política puede utilizarse para disciplinar, y tal vez despedir, a un trabajador que realice actividades de "hacking" con los sistemas informáticos de la Empresa X. Esto es deseable si la organización quiere evitar que esta actividad se revele al público.

Políticas Relacionadas: "Prueba de los Controles del Sistema Informático" y "Evidencia de Delito o Abuso Informático"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

2. Regulación del Software

Política: Todo el software instalado en los sistemas multiusuarios de la Empresa X, debe estar regulado por un sistema aprobado de control de acceso que controle la sesión de un usuario antes de entregar el control a otro software de aplicación.

Comentario: Esta política impide la instalación de un software que no pueda ser regulado por un sistema de control de acceso. El software para el sistema de control de acceso no necesita ser un sistema operativo. Puede ser un paquete de control de acceso por niveles o tal vez un módulo de interface o un cortafuegos que lleve a cabo el control del acceso. Esta política es menos necesaria en sistemas operativos, en los que todas las solicitudes de servicio son mediadas automáticamente por los mecanismos de control de acceso de los sistemas operativos. Algunos de los sistemas operativos más tradicionales necesitan una política como ésta. La política no está diseñada específicamente para los sistemas operativos; además, indirectamente prohíbe que los programadores instalen puertas falsas y demás software que puedan burlar un sistema de control de acceso. Esta política habitualmente sería enviada sólo a los programadores y administradores de sistemas y al personal de soporte técnico asociado.

Políticas Relacionadas: "Mal Funcionamiento del Control de Acceso" y "Autentificación del Usuario por el Sistema Operativo"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Control de Acceso Basado en Contraseña

Política: Cualquier sistema pequeño que maneje información bien sea crítica o sensible, debe utilizar una versión mantenida adecuadamente de un sistema de control de acceso basado en contraseñas.

Comentario: Esta política proporciona a los administradores de sistemas pequeños una guía específica en cuanto al uso de un sistema de control de acceso basado en contraseñas. Aquellos sistemas que no contengan información crítica o confidencial, no tienen en forma

predeterminada que poseer un sistema de control de acceso. Las palabras "mantenida adecuadamente" se incluyeron en la política para dar a entender que la simple instalación de un paquete no es suficiente. En algunos casos, el paquete puede ser instalado, pero puede que no se use para proteger archivos confidenciales o críticos. Esta política asume que las palabras "sensible" y "crítica" han sido formalmente definidas. La palabra "valiosa" se puede añadir a esta política.

Políticas Relacionadas:“[Clasificación de Datos en Cuatro Categorías](#),” “[Control de Acceso a Computadores de Red](#),” y “[Control de Acceso Físico a la Información Sensible](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

4. Acceso de Lectura a Información Sensible

Política: Los trabajadores que han sido autorizados para ver la información clasificada con un cierto nivel de sensibilidad, pueden acceder sólo a la información de ese nivel o a la de menor nivel de sensibilidad.

Comentario:Esta política gira instrucciones a los administradores de sistemas y a los otros que establecen los privilegios de control de acceso, en el sentido de evitar que los usuarios obtengan acceso no autorizado a la información. Por ejemplo, una persona que ha sido autorizada para ver información Secreta también puede ver la información Pública y la Confidencial, ya que éstas son menos sensibles que la información secreta. Esta persona, sin embargo, no puede ver la información altamente secreta, a menos que se le haya otorgado una autorización específica. A este enfoque se le denomina "leer hacia abajo" o "no leer hacia arriba", ya que al usuario se le ha permitido leer sólo hasta su nivel de clasificación y de esos niveles hacia abajo, que progresivamente se tornan menos sensibles. Esta política se aplica a todos los niveles de datos, sin importar cuántos niveles existan en un sistema de clasificación. Por ejemplo, si un usuario sólo tiene permiso para leer datos "no clasificados" o los de nivel menos confidencial, entonces el usuario no puede tener acceso a otros niveles. Contrariamente, si una persona tiene acceso al nivel de datos más alto, esta persona puede acceder a todos los demás niveles. Esta política se observa más a menudo en organizaciones militares y diplomáticas, mientras que las organizaciones comerciales generalmente utilizan modelos menos complejos. Desafortunadamente un número cada vez mayor de

sistemas operativos comerciales no respaldan esta política. Es necesario un software adicional para la puesta en práctica de la política.

Políticas Relacionadas:“[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

5. Acceso de Escritura a Información Sensible

Política: Los trabajadores no deben trasladar la información clasificada con un cierto nivel de sensibilidad a un nivel de menor sensibilidad, a menos que esta acción forme parte de un proceso de degradación autorizado.

Comentario:Esta política prohíbe a los usuarios que muevan los datos de un nivel de clasificación a otro, a fin de poder obtener acceso no autorizado. Por ejemplo, si una persona pudiera copiar información "altamente secreta" y lo transfiriera a "confidencial", un archivo menos sensible, la persona le estaría dando acceso a otra persona que de otro modo no estaría autorizado para ver dicha información. El proceso de escribir información en un nivel de clasificación menos sensible puede considerarse como de degradación de la información, de tal manera que entes no autorizados puedan tener acceso a la misma. Algunas organizaciones querrán añadir palabras a esta política, describiendo las maneras en que los usuarios pueden tener conocimiento de que el proceso de desclasificación ha sido autorizado. En general, esta política es común en las organizaciones militares y diplomáticas en vez de en las organizaciones comerciales. La política se puede aplicar automáticamente, aunque la mayoría de los sistemas operativos comerciales no la apoyen. Se requiere de un software adicional para su puesta en práctica.

Políticas Relacionadas:“[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

6. Permisos Predeterminados de Archivo

Política: Los permisos para el control de acceso de los archivos para todos los sistemas en red de la Empresa X, se deben establecer de forma predeterminada para que bloquee el acceso a los usuarios no autorizados.

Comentario: Esta política proporciona una guía tanto a los usuarios como a los administradores de sistemas, para el establecimiento de los controles de acceso apropiados para los sistemas en red. Los sistemas de computación que no están conectados en red, generalmente necesitan menos controles de acceso lógico ya que pueden apoyarse en medidas de seguridad física, como la cerradura de una puerta de oficina. Esta política está escrita de tal manera que sólo se aplique a los sistemas en red. Algunos integrantes del personal a menudo deciden por sí mismos que los controles de acceso lógico consumen tiempo y recursos. Esta política prohíbe al personal tomar decisiones que pueden no estar dentro de los intereses de la organización en el largo plazo. La política también puede resultar útil en casos donde la administración local no quiere gastar dinero en la definición de los controles de acceso. La política requiere que ellos apoyen al personal técnico que realiza estas tareas.

Políticas Relacionadas: “Privilegios Predeterminados de Usuario,” “Mal Funcionamiento del Control de Acceso,” y “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

7. Mal Funcionamiento del Control de Acceso

Política: Si un sistema de control de acceso de una computador o red no está funcionando de manera adecuada, debe negar de manera predeterminada los privilegios a los usuarios finales.

Comentario: En vez de permitir un acceso abierto y sin control, la presente política evita dicho acceso hasta que el sistema de control de acceso sea reparado. Por ejemplo, si un sistema de control de acceso basado en contraseñas de un servidor web presentara mal funcionamiento, no se debería permitir el acceso al sistema a ningún usuario final, pero el personal técnico requeriría tener acceso para poder arreglar el problema. Algunas organizaciones querrán agregar ciertas exclusiones específicas a la política, para mantener en condición operativa los procesos comerciales esenciales, tales como la cobranza de cheques en un banco. Todas estas exclusiones deben considerarse con sumo cuidado antes de incorporarlas a la política, porque pueden correr el riesgo de convertirse en áreas explotadas por espías industriales, estafadores y otras personas implicadas en abusos de sistemas informáticos. En líneas generales, si reflejan con precisión el medio ambiente, lo deseable es

que políticas como éstas se mantengan sencillas y directas. Las excepciones deben hacerse en forma particular.

Políticas Relacionadas: “Capacidad de Acceso de Usuarios” y “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Base de Datos Centralizada de Controles de Acceso

Política: Los registros no ambiguos, organizados y actualizados de todos los privilegios de acceso al sistema informático de producción, se deben mantener en una base de datos centralizada que esté en manos de la Administración de Seguridad Informática.

Comentario: Esta política garantiza que el departamento de Seguridad Informática estará al tanto de todos los cambios que se produzcan en los privilegios de los usuarios que tengan acceso a los sistemas de producción de la Empresa X. Los administradores de sistemas de otros departamentos, o incluso el personal de una organización externa, pueden realizar los cambios; no obstante, se debe informar de inmediato de estos cambios a la administración de Seguridad Informática. Una base de datos centralizada para el control de acceso permite que todos los privilegios del trabajador saliente sean eliminados de inmediato, lo cual es muy importante en despidos traumátizantes cuando la persona es escoltada hacia la puerta en circunstancias poco deseables. Por ejemplo, alguien pudo haber sido capturado por estafar a la organización. En estos casos, es posible que se produzca una situación de venganza, y es por eso que es tan importante que todos los privilegios que estén a la disposición del trabajador saliente cesen de manera inmediata y definitiva. No existe posibilidad alguna de que este objetivo se cumpla de manera confiable sin una base de datos centralizada de todos los privilegios. También se pueden utilizar las bases de datos centralizadas para ejecutar determinadas aplicaciones de software que puedan detectar conflictos de intereses, excesivos privilegios y otros problemas que no hayan llamado la atención de los administradores del sistema. A veces, los sistemas de software que sirven de apoyo a una base de datos centralizada reciben el nombre de Sistemas para la Administración de la Seguridad Empresarial.

Políticas Relacionadas: “Cambios en Situación del Trabajador”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

9. Software Intérprete de Líneas de Comando

Política: Se debe eliminar todo software de interpretación de líneas de comandos de aquellos computadores que no lo requieran, a fin de que realicen el procesamiento normal.

Comentario:Esta política instruye al personal que trabaja en el área de programación de sistemas con el fin de eliminar aquel software que responda al comando introducido desde un teclado, en contraposición de aquel comando que podría indicarse haciendo click con el ratón en un botón de una pantalla tipo explorador, o a través de un ratón que selecciona entre varias opciones predeterminadas de un menú. Los privilegios de línea de comando permiten detener el procesamiento de los sistemas, modificar los privilegios de control del acceso, desactivar los registros de entrada y otras acciones que pudieran tener un impacto material en la seguridad de un sistema de producción. En caso de que el software de interpretación de líneas de comandos no se encuentre disponible, se impedirán en gran medida los esfuerzos de los intrusos por obtener la mayor condición de privilegio de un sistema. Esta política no significa que es necesario obstaculizar o producir molestias de cualquier tipo al personal que trabaja en el área de operaciones computarizadas, pero sí supone que dichas operaciones han sido registradas de tal modo que se puedan realizar todas las acciones normales, sin necesidad de agregar una línea de comando. Esta política puede emplearse para disminuir los errores y omisiones provocadas por el personal de operaciones computarizadas y, dado que algunos comandos no están a su disposición, se disminuye el riesgo de que ocasionen un daño grave. Antes de adoptar esta política, la organización debe garantizar que su respuesta ante emergencias y sus procedimientos para recuperarse de un desastre no requerirán de un dispositivo de interpretación de líneas de comando.

Políticas Relacionadas:“Software Innecesario” y “Computadores para Cortafuegos”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

10. Burlado de los Controles de Acceso

Política: Los programadores y demás personal técnico deben abstenerse de instalar cualquier código que bloquee los mecanismos autorizados de control de acceso que se encuentran en los sistemas operativos o en los paquetes de control de acceso.

Comentario:Las trampas son segmentos especiales de código que permiten a un programador de sistemas, a un miembro del personal de apoyo técnico o a alguna otra persona obviar o bloquear los controles de acceso normales. Estas partes ocultas del código se invocan mediante comandos especiales no documentados que sólo conoce la persona que lo escribió. Es irónico que la mayoría de las trampas se instalan con buenas intenciones, tales como poder instalar código de mantenimiento del sistema sin reiniciar el computador, poder emitir comandos de programación de sistemas privilegiados desde los terminales de un usuario cualquiera, o poder obviar el sistema de control del acceso, en caso de que éste colapse. Esta política requiere que todos los accesos se sometan a mecanismos normalizados de control de acceso, con lo cual se logrará uniformidad, auditabilidad y un ambiente operativo más seguro. Si existen las trampas, personas no autorizadas podrían utilizarlas para dañar el sistema; asimismo, si la persona que instaló las trampas abandona la organización en condiciones menos que amigables, dicho ex-trabajador podría ocasionar un daño grave a través de las trampas. Esta política se podría modificar para aplicarla a controles de acceso a los sistemas de las aplicaciones o a los controles de acceso al sistema de administración de las bases de datos y a los controles de acceso que se encuentran en los sistemas operativos y en los paquetes de control de acceso.

Políticas Relacionadas:“Autentificación del Usuario por el Sistema Operativo” y “Vías de Acceso en Software de Producción”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

11. Comprometer Mecanismos de Seguridad para los Clientes

Política: No deben aceptarse las solicitudes de clientes que comprometan los mecanismos de seguridad de la Empresa X, salvo que el vicepresidente ejecutivo lo apruebe por escrito o la Empresa X se vea obligada a hacerlo por requisito de ley.

Comentario: Esta política se encarga del balance que debe existir entre el servicio que debe recibir el cliente y la seguridad que debe mantener la empresa. Por ejemplo, una empresa que produce software para procesadores de palabras con cifrado puede recibir la solicitud de un cliente para que disuelva el proceso de cifrado, de modo que se pueda descifrar la única copia disponible de un archivo. La política indica que la empresa fabricante del software no debe realizar tal práctica, salvo que se cumplan una o ambas condiciones establecidas en la misma. Si la empresa fabricante de software comprometía a menudo el proceso de cifrado, se pudiera correr la voz de que la empresa puede hacerlo y que lo hará. En consecuencia, se le solicitaría a la empresa realizarlo regularmente; asimismo, la empresa tendría que determinar si el solicitante tenía la autoridad adecuada para hacer tal solicitud. La política no incluye la puesta en riesgo de los controles que se encuentran en los sistemas externos de la Empresa X, pero ciertas organizaciones pueden extender el ámbito de esta política hasta los sistemas externos. Por ejemplo, esto evitaría que un intermediario informático comprometiera los controles de un sistema externo con el fin de obtener cierta información que le interesa.

Políticas Relacionadas: “Código Fuente del Software de Penetración de Sistemas,” “Vías de Acceso en Software de Production,” “Enunciados de la Integridad del Software,” y “Prueba de los Controles del Sistema Informático”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

12. Restricciones a la Recopilación de la Información

Política: Si la información sensible de la Empresa X se encuentra en un sistema de computación y si se permite a los usuarios solicitar esta información en parte o en su totalidad a través de instalaciones en línea, se deben establecer controles de acceso especiales para proteger la información, de modo que la serie de solicitudes de información permisibles no revelen de manera colectiva alguna información que esté restringida.

Comentario: Esta política asigna ciertos lineamientos a las personas encargadas de la seguridad para establecer sistemas de control del acceso. Por ejemplo, un administrador de redes que se encuentre estableciendo un sistema de control de acceso podría beneficiarse de una política parecida. Asimismo, un programador que construya una instalación destinada a manejar bases de datos montadas en un servidor público al que se pueda

acceder a través de Internet, debe recordar la existencia de esta política. La presente política indica que se deberían definir los privilegios en el control de acceso en categorías amplias, tales como los cargos en una empresa, en vez de categorías detalladas tales como los datos sobre las personas. El término "sensible" puede sustituirse por una designación como "secreto", a fin de mantenerse a tono con la política interna de clasificación de datos.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Información Estadística de los Registros de los Clientes,” “Asignación de Etiquetas de Clasificación de Datos,” y “Etiquetado de Clasificación Múltiple”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

13. Divulgación de la Información de Terceros

Política: Los trabajadores de la Empresa X no deben divulgar ninguna información sensible que le haya sido confiada a través de terceros a otras terceras personas, salvo que la persona que originó la información haya dado su aprobación con antelación en lo referente a su divulgación, y que la parte que reciba dicha información haya firmado un acuerdo de confidencialidad.

Comentario: Debido a que hoy en día las sociedades comerciales son más frecuentes, a menudo se comparte información confidencial entre empresas. Pero, antes de compartir la información, las organizaciones que la originan deben sentir confianza en el sentido de que su información no va a ser divulgada a terceros desconocidos. Para ayudar a generar esta confianza, esta política establece claramente que la Empresa X exigirá un acuerdo de confidencialidad y una autorización previa antes de que cualquier tercero obtenga la información que ha sido confiada a la Empresa X. Para que esta política sea realmente eficaz, será necesario etiquetar la información, de modo que la persona u organización que la origine sea fácilmente identificable, o si no, ofrecer otras facilidades, tales como un diccionario de datos corporativos que identifique a la persona u organización que origine los mismos.

Políticas Relacionadas: “Divulgación de Información Privada a Terceros,” “Acuerdos de Confidencialidad,” y “Solicitudes Externas de Información”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

14. Solicitudes de Información Organizacional

Política: Todas las solicitudes de información sobre la Empresa X y sus actividades de negocios, incluyendo, sin limitantes, cuestionarios, sondeos y entrevistas periodísticas, deben ser referidas al departamento de Relaciones Públicas, a menos que la alta gerencia lo autorice.

Comentario: Esta política evita que los trabajadores, sin importar sus intenciones, divulguen información sensible a la prensa, investigadores de mercado, competencia, espías industriales, hackers y otros. Esta política autoriza únicamente al departamento de Relaciones Públicas o a los voceros designados - a menudo expertos en la materia - a divulgar información sobre la Empresa X y sus actividades comerciales. Al concentrar la divulgación a través del departamento de Relaciones Públicas, la organización está también en la capacidad de presentar al público una imagen coordinada y ordenada; lo cual también reducirá las probabilidades de que los espías industriales utilicen la ingeniería social para extraer información de empleados desprevenidos. Esta política es importante después de un siniestro o de algún problema que haya sido divulgado en público. En estas circunstancias, la prensa andará en la búsqueda de empleados para entrevistarlos. Cuando esto ocurra, si las divulgaciones no son manejadas con sumo cuidado, la organización puede dar una imagen de estar deficientemente administrada y confundida. Esta política puede formar parte de los esfuerzos de planificación en casos de contingencia dirigidos a lo que se debe hacer en caso de explosiones de bombas, sismos, y otros desastres y emergencias. Muchos empleados se sentirán aliviados al contar con una propuesta sencilla para deshacerse en forma educada de las personas que soliciten información. En algunas organizaciones, el departamento de Relaciones Públicas puede tener voceros designados para hablar sobre ciertos temas; por ejemplo, si se ha producido un problema de seguridad informática, el director del departamento de Seguridad Informática puede estar autorizado a dirigirse al público. En pocas palabras, ciertas organizaciones querrán agregar las palabras "y sistemas informáticos" luego de "actividades de negocios".

Políticas Relacionadas: "Liberación de Información de la Organización," "Seguridad Informática Centralizada," y "Presentación de la Imagen Pública"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

15. Divulgación de Información de Negocios del Cliente

Política: Los trabajadores de la Empresa X no deben divulgar a ninguna persona ajena a la Empresa X la naturaleza de los proyectos del cliente, sus estrategias empresariales o sus relaciones comerciales.

Comentario: Esta política sirve de advertencia a las organizaciones, al momento de divulgar cierta información sobre los clientes. Esto sería de gran importancia para, por ejemplo, una organización de consultoría que realizara investigaciones sobre fraudes. La política es estricta en el sentido de que no permite divulgación de información alguna, aun cuando se mantenga oculta la identidad del cliente. El ámbito de esta política podría expandirse para incluir el modo en que esto funciona con un cliente en particular. Los comentarios que se hagan a los reporteros, tales como "se nos hace difícil trabajar con ellos", pueden dañar las relaciones actuales, incluso cuando no divultan, en el sentido más estricto de la palabra, información sensible.

Políticas Relacionadas: "[Compartir Información de Mercadeo](#)" y "[Comunicaciones Públicas](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

16. Compartir Información de Mercadeo

Política: No se debe divulgar jamás a la competencia información de mercadeo, incluyendo, sin limitaciones, precios, políticas de ventas, estrategias, planes, segmentos de mercado y otra información sobre el área de mercadeo.

Comentario: Esta política aclara lo que a menudo resulta ser un punto de confusión para las personas que trabajan en el área de ventas y mercadeo. Por un lado, se discuten con un cliente potencial las políticas de precios y ventas y, por otro, esta información es sumamente valiosa para la competencia. Por supuesto que los terceros que trabajan para la competencia podrían reunir esta información a nombre de ella, pero esta política requiere que la competencia se comprometa a realizar una actividad que bordea en lo poco ético. El simple hecho de que esto sea cuestionable no significa que la competencia no utilizará a terceros para recolectar información de inteligencia competitiva, por lo que esta política les complicará la cosa. La política supone que las personas que trabajan en el área de ventas y mercadeo saben quiénes son su competencia. Existen tantos competidores en ciertas industrias que no es

posible tener un listado actualizado de todos ellos. Cada una de las organizaciones querrá especificar de manera explícita los tipos de información que desea ocultar.

Políticas Relacionadas: “[Acuerdos de Confidencialidad con Antiguos Patronos](#)” y “[Renuncia de Empleados por la Competencia](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Información Liberada al Público — Nombre del Contacto

Política: La información generada por la Empresa X y dada a la luz pública debe estar acompañada del nombre del integrante del personal designado para actuar como única fuente oficial reconocida y único contacto.

Comentario: Esta política proporciona un enfoque organizado para la divulgación de la información, garantiza una posición consistente con respecto a la misma y desarrolla un mecanismo que controla las distintas formas en que se puede presentar al público. Depende más de fuentes designadas que del departamento de Relaciones Públicas para proporcionar cierto orden a este proceso. La política se podría modificar para declarar que únicamente el Propietario designado de la información puede sacarla a la luz pública porque, ya que existen computadores en prácticamente todos los escritorios, cualquier trabajador es un editor en potencia. Ciertas organizaciones querrán especificar algunas excepciones a la política, tales como los folletos de mercadeo.

Políticas Relacionadas: “[Aprobación de las Representaciones Públicas](#)” y “[Solicitudes Externas de Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Información de Asuntos Legales

Política: No debe satisfacerse ninguna solicitud de información por parte de terceros relacionada con un caso legal actual, a menos que la solicitud sea efectuada por un organismo gubernamental autorizado.

Comentario: Esta política evita que el personal de la Empresa X haga comentarios inapropiados o suministre información relacionada con asuntos que se encuentran ya en los tribunales y que perjudican al caso de algún

modo. Por ejemplo, esto podría ocurrir si el empleado de la Empresa X suministrase cierta información básica que la contraparte desconoce. Si esta información llegase a salir publicada en el artículo de algún periódico, el abogado de la contraparte podría utilizarla. La política no prohíbe que los integrantes del personal respondan a los procedimientos de la fiscalía, las citaciones y otras solicitudes legítimas de información en lo referente a algún asunto que se esté sometiendo a litigio. Nada de lo contenido en esta política evita que la gerencia divulgue a los medios noticiosos cierta información selectiva que considere de ayuda para obtener apoyo público para un asunto legal ya en desarrollo.

Políticas Relacionadas: “[Información Liberada al Público — Nombre del Contacto](#),” “[Uso del Nombre de la Organización](#),” y “[Solicitudes de Información Organizacional](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Liberación de Información de la Organización

Política: Se debe obtener permiso previo de la gerencia principal de la Empresa X para divulgar cualquier información interna de la misma a los medios noticiosos o a otros terceros.

Comentario: Esta política evita que los empleados divulguen información sensible a la prensa, investigadores de mercado, competencia, hackers y otros. Queda prohibida la divulgación de la información sin una autorización explícita. Debido al hecho a que se utiliza el término “interna”, la política no abarca cierta información pública. El término “interna” podría sustituirse por “sensible” o “clasificado”, ya que esta política no requiere que toda la información fluya a través de punto de compensación central. Con esta propuesta se corre el riesgo de presentar ante el público una imagen de empresa deficientemente administrada y desorganizada. Una opción que se puede agregar a esta política incluiría la obtención de un permiso gerencial por escrito antes de cada publicación.

Políticas Relacionadas: “[Solicitudes de Información Organizacional](#),” “[Presentación de la Imagen Pública](#),” y “[Entrega de Documentación de Sistemas](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

20. Ganancias o Productos Futuros

Política: Los empleados no deben hacer ningún tipo de representación pública sobre las ganancias a futuro de la Empresa X o las posibilidades que existan de nuevos productos.

Comentario: La proliferación de recientes demandas grupales ha preocupado a la gerencia principal de muchas organizaciones en torno a las repercusiones de hacer proyecciones a futuro y, por eso, esta política prohíbe cualquier declaración pública al respecto. Además, la política no sólo ayudará a detener las demandas contra los inversionistas, sino que también ayudará a disminuir las fluctuaciones en los precios de las acciones ocasionadas por los resultados financieros reales que no se compaginan con las proyecciones financieras publicadas. Esta política tiene relevancia sólo para las empresas que realizan transacciones bursátiles públicas; mientras que aquéllas que no las realizan no requieren de una política como ésta. Esta política tiene que ver con las representaciones verbales efectuadas a reporteros y con la representación escrita efectuada en las posibles ofertas de acciones, informes anuales y documentos relacionados. Es posible que ciertas organizaciones califiquen a esta política como demasiado estricta y querrán agregar la frase "con la excepción de la gerencia ejecutiva" después del término "trabajadores".

Políticas Relacionadas: "[Solicitudes de Información Organizacional](#)" y "[Comunicaciones Públicas](#)"

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

21. Solicituds Externas de Información

Política: Todas las solicitudes de información interna provenientes de terceros que no tenga como origen el departamento de ventas, mercadeo o relaciones públicas, deben ser aprobadas por el Propietario de la información y el asesor legal corporativo, quienes contarán con un plazo de cinco días hábiles para evaluar los méritos de la solicitud.

Comentario: Esta política define las formas de manejar las solicitudes externas de información interna que pudiera estar restringida; por ejemplo, la información pudiera violar la privacidad de una determinada persona, ser información relacionada con la defensa nacional, estar requerida mediante mandato de ley para realizar una investigación en desarrollo o por alguna

otra razón por la cual no pudiera ser conveniente divulgarla. Esa posibilidad es la razón detrás del período de revisión de cinco días. Las organizaciones comerciales podrían hacer uso de esta política, si ésta se restringiera a determinada información que el público tuviera el derecho de recibir. Por ejemplo, en una empresa de servicio eléctrico se podría divulgar al público información sobre los sistemas que se utilizan para la generación de electricidad, en ausencia de objeción de las partes nombradas en dicha política. Cuando se utiliza en un organismo gubernamental, la referencia que hace esta política de la facultad que tienen las partes para vetar la solicitud, podría pasar a manos de los gerentes de nivel medio a cargo de los sistemas y de la información relacionada con éstos.

Políticas Relacionadas: "[Solicitudes de Información Organizacional](#)"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

22. Información Sensible Controversial

Política: La información sensible y controversial de la Empresa X debe salir a la luz pública por entregas.

Comentario: Esta política garantiza que una explicación intencional de la Empresa X irá acompañada de cada información controversial publicada, lo cual disminuye el daño a la reputación de la Empresa X y ayuda a garantizar que la información será utilizada para los fines destinados. El proceso que presenta esta política para publicar información controversial puede ocasionar un conflicto con las órdenes de un tribunal; aunque en este caso prevalecerían las órdenes tribunalicias. Sin embargo, si la empresa publicase la información de manera voluntaria para beneficiar al público o para ayudar a algún grupo sin fines de lucro, entonces se aplicaría esta política. Este enfoque le da tiempo a la organización para investigar sus registros internos y determinar toda la información que va a ser publicada. El enfoque permite a la Empresa X publicar primero las partes menos controversiales de la información sensible recolectada y, luego gradualmente, proporcionar el material más controversial.

Políticas Relacionadas: "[Presentación de la Imagen Pública](#)" y "[Solicitudes de Información Organizacional](#)"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

23. Avisos Solicitando Empleados

Política: La gerencia de Recursos Humanos debe aprobar con antelación todos los avisos o anuncios públicos en los que se soliciten ayudantes, antes de su publicación.

Comentario: Esta política evita que los analistas de inteligencia competitiva utilicen los avisos donde se solicitan ayudantes para determinar qué hacen las demás empresas y cuáles son los nuevos productos que saldrán al mercado. Estos avisos pueden sacar a la luz pública las prioridades que tiene la gerencia y los problemas internos de la empresa; además, pueden indicar la dirección estratégica de una organización. Se recomienda no mencionar el nombre de la empresa en ninguna parte del aviso. Algunas organizaciones podrían ir más allá, rotando la información de contacto, tales como el número telefónico o de fax. Normalmente, los reclutadores de personal mantienen oculto el nombre de sus clientes hasta saber que tienen un buen candidato, debido a que los demás podrían utilizar esta información con fines desconocidos y no autorizados.

Políticas Relacionadas: “[Comunicaciones Públicas](#)” y “[Solicitudes Externas de Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

24. Información Liberada al Público — Autorización

Política: La gerencia debe revisar toda información a publicarse, de acuerdo con un proceso establecido y documentado.

Comentario: Esta política requiere que la gerencia establezca y observe un procedimiento formal para revisar la información antes de su publicación. Más allá de exigir tal procedimiento, esta política requiere, asimismo, que el procedimiento esté documentado. La política puede expandirse para requerir que se genere la documentación de cada una de las solicitudes. Quizás la parte más importante de este último tipo de documentación es la correspondiente a las autorizaciones específicas suministradas. Es probable que la existencia de la documentación dé como resultado decisiones bien argumentadas. A pesar de ser adecuada para aquellas organizaciones que cuentan con esquemas de clasificación de datos altamente desarrollados, esta política puede igualmente existir en ausencia de un esquema formal de clasificación de datos.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)” y “[Liberación de Información de la Organización](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

25. Comunicaciones Públicas

Política: Todo discurso, presentación, documento técnico, libro o comunicación a distribuirse al público debe contar con la autorización de publicación correspondiente emitida por el jefe inmediato del empleado involucrado.

Comentario: Esta política requiere que los empleados obtengan siempre la autorización de sus gerentes antes de pronunciar un discurso, hacer una presentación, entregar un documento u otro tipo de comunicación, lo cual evita la divulgación no autorizada de información sensible. En el caso de que un empleado disertara sobre la condición general de la industria en la que la Empresa X ofrece sus productos o servicios, también requeriría de autorización. Esta política podría incluir la frase “los trabajadores no deben divulgar más información de la Empresa X que la necesaria para alcanzar el objetivo deseado”. Es de particular preocupación la divulgación pública del material que aún no se haya patentado. Si esta información se publica antes del registro de la patente, ésta puede quedar invalidada, puesto que las leyes sobre patentes varían de un país a otro.

Políticas Relacionadas: “[Aprobación de las Representaciones Públicas](#)” y “[Liberación de Información de la Organización](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

26. Autorización de Divulgación de Información

Política: La divulgación de cualquier archivo almacenado y todo mensaje enviado a través de la red de la Empresa X a terceros debe estar precedida de una revisión y una autorización por parte del director del departamento legal.

Comentario: Esta política informa a los usuarios que no deben crearse expectativas acerca de su privacidad al momento de utilizar los sistemas informáticos de la empresa. Esta política garantiza que esta información jamás será compartida con personas ajena a la empresa, pero sólo si cuenta con la autorización del director del

departamento legal. Esta intención servirá para evitar problemas de responsabilidad civil; por ejemplo, la persona involucrada pudiera afirmar que la divulgación de dicha información era poco halagadora y que ha sido dañada su reputación, o afirmar que los hechos están errados y que ha sido calumniada. Un buen procedimiento para evitar o reducir la exposición a estos problemas es lograr que un experto legal revise la divulgación de esa información.

Políticas Relacionadas: “[Información Liberada al Público — Autorización](#)” y “[Acuerdos de Confidencialidad — Organización](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

27. Naturaleza y Ubicación de la Información de la Organización

Política: La información relativa al origen y ubicación de la información sobre la Empresa X, por ejemplo la que se encuentra en un diccionario de datos, es confidencial y debe divulgarse únicamente a aquellas personas que tengan una necesidad demostrable de conocerla.

Comentario: Esta política notifica a los trabajadores que la información sobre la información, también denominada metadata o metadatos, es confidencial. La diferencia que se presenta aquí está entre restringir el acceso a la información basándose en la necesidad de conocerla y restringir el acceso a la información sobre la información basándose en la necesidad de conocerla. Los metadatos son de gran utilidad para los hackers, espías industriales, saboteadores y otros que intenten ocasionar daño a la Empresa X. En muchos casos los metadatos son más valiosos que la información a la cual se refieren, debido a que los metadatos pueden incluir una etiqueta de clasificación de datos, una descripción de importantes medidas de control, los sistemas en los cuales reside la información y las personas que tienen derechos de acceso legítimo a la información. Desde el punto de vista comercial, la información sobre la existencia de un producto o servicio que pronto saldrá al mercado puede ser de mayor importancia que las especificaciones reales del producto. Si bien los diccionarios de datos pueden ser herramientas gerenciales importantes, el acceso a la información contenida en los mismos debe restringirse de acuerdo con la necesidad de conocerla. Asimismo, los sistemas de administración de documentos contienen metadatos que deben restringirse de conformidad con esta política.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#),” “[Atributos de la Integridad de la Información](#),” e “[Inventario de Activos — Información](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

28. Exploración de Sistemas

Política: Los empleados no deben explorar los sistemas informáticos o redes de la Empresa X.

Comentario: Esta política prohíbe las actividades de exploración o violación de la información. En muchos casos, los perpetradores de abusos informáticos tienen más curiosidad que malicia deliberada pero a menudo sacan provecho de la información que descubren. Al ser atrapadas, estas personas dicen con frecuencia que sólo estaban explorando y no tenían malicia o intenciones de cometer actos fraudulentos. Para contrarrestar dichas afirmaciones, esta política establece claramente que no es aceptable la exploración de los sistemas informáticos. Si los trabajadores exploran la red de la Empresa X, esta política brinda a la gerencia una herramienta con la cual disciplinar o dar por terminada la relación laboral con estos trabajadores. La política tiene una importancia particular para los computadores personales, los terminales, los sistemas cliente-servidor y las redes de área local, debido a que estos pequeños sistemas presentan a menudo controles de acceso inadecuados. Esta política no es un sustituto aceptable de un sistema de control de acceso real. Se podría expandir la política para incluir la navegación en la intranet, lo cual es permisible y no se considera exploración.

Políticas Relacionadas: “[Errores y Manipulación de Registros](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

29. Madurez del Producto de Seguridad

Política: Los productos de seguridad con menos de un año en el mercado no deben emplearse como componentes integrales de cualquier sistema informático de producción crítica para la Empresa X.

Comentario: Esta política evita que los diseñadores de sistemas u otros utilicen productos de seguridad muy nuevos para los sistemas de producción. Nada de lo establecido en esta política impide a la Empresa X actuar como sitio beta o probar estos nuevos productos.

Sin embargo, si evita que la Empresa X dependa de esos productos. La principal preocupación existente aquí es el descubrimiento de deficiencias en materia de seguridad que más tarde puedan ocasionar una situación vergonzosa para la organización, obligar a la descontinuación de los sistemas de producción involucrados o permitir la comisión de delitos como el fraude. Si espera un año, la Empresa X se entera a través del mercado de los problemas más importantes que presenta el producto. Aunque es poco común, también se podría aplicar esta política, o una política derivada con menor exigencia en lo relativo al lapso de tiempo, a versiones importantes de productos de seguridad utilizados en los sistemas informáticos. Para las empresas más conservadoras, esta política podría aplicarse a todos los productos de sistemas informáticos, y no sólo a los productos de seguridad. Si, tal como está definida, la política pareciera demasiado estricta, se puede proporcionar un proceso de autorización especial para manejar las excepciones.

Políticas Relacionadas: “Versiones de Sistemas Operativos”, “Herramientas y Técnicas de Desarrollo Maduras”, y “Arreglos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

30. Creación de Herramientas de Seguridad

Política: Los desarrolladores y diseñadores de los sistemas internos de la Empresa X no deben crear nuevos protocolos de seguridad, componer nuevos esquemas de seguridad, desarrollar nuevos algoritmos de cifrado o, de modo alguno, volverse creativos en lo relativo a la seguridad informática.

Comentario: Esta política está dirigida a resolver un problema grave de la comunidad de desarrolladores de sistemas. Muchos programadores, diseñadores de sistemas y otros que desarrollan sus propios esquemas, protocolos y métodos de seguridad, no cuentan con la pericia adecuada para llevarlos a cabo. Debido a que no comprenden los riesgos relacionados, a menudo lo que hacen es crear problemas para sus organizaciones. El objetivo de esta política es evitar que los desarrolladores utilicen nuevas aplicaciones o nuevos sistemas a manera de proyectos personales. Más bien, entonces, la política reitera que la seguridad es un asunto serio y que deben utilizarse las prácticas y métodos probados y aceptados.

Políticas Relacionadas: “Algoritmos de Cifrado Evaluados Públicamente” y “Algoritmo de Cifrado Normal e Implementación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

31. Facilidad de Uso de los Controles de Seguridad

Política: Todas las medidas de seguridad aplicadas a equipos de computación y de comunicaciones deben ser simples y de fácil uso, administración y auditoría.

Comentario: Esta política exige que todos los controles aplicados a los computadores y a las comunicaciones sean prácticos y sostenibles. Si las medidas de seguridad son demasiado complejas, es posible que sean malentendidas, malinterpretadas o incorrectamente aplicadas. En aquellos casos en que los controles resulten difíciles de manejar, engorrosos o, de algún modo, mal diseñados, los usuarios los pasarán por alto o los rechazarán. Esta política reconoce la realidad en el sentido de que, para que los controles funcionen, debe existir un equilibrio entre los objetivos de seguridad y los aspectos prácticos, tales como costo y facilidad de manejo. En esta política se puede utilizar el término “amigable”, pero se ha utilizado tanto que ya ha perdido buena parte de su significado. A fin de que la política sea más clara, ciertos lectores querrán eliminar dos de las tres instancias en las que aparecen las palabras “simple y fácil”. Esta política está dirigida a diseñadores e integradores de sistemas y otras personas cuya misión es instalar sistemas informáticos. Nada de lo aquí contenido impide a los diseñadores construir sistemas complejos. La política sólo exige que dicha complejidad se mantenga oculta de los usuarios y de otras personas que deban interactuar con el sistema.

Políticas Relacionadas: “Controles Mínimos en Sistemas Informáticos” y “Aceptación del Usuario de las Medidas de Seguridad Informática”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

32. Uso de Derechos en Sistemas Informáticos

Política: No deben utilizarse los derechos en sistemas informáticos para cualquier propósito empresarial de la Empresa X hasta obtener la autorización escrita del gerente de Seguridad Informática.

Comentario: Esta política es una expresión de lo que se denomina diseño restringido, cuyo objetivo es evitar que los privilegios habilitados, pero no suficientemente

examinados, sean utilizados por intrusos y otras personas no autorizadas. Por ejemplo, según la configuración de un cortafuego, se permitirán ciertos servicios en internet y se prohibirán otros. A menudo, los proveedores despachan los productos con muchos, cuando no todos los servicios permitidos, lo cual permite a los clientes poner los sistemas en funcionamiento con bastante rapidez. Igualmente, la Internet está diseñada con una propuesta de diseño permisiva que establece que se permite todo lo que no está específicamente prohibido. Esta política impone cierto grado de inflexibilidad, debido a que los cambios de privilegios deben ser aprobados con antelación, pero garantiza que los servicios que no hayan sido investigados adecuadamente no serán utilizados en contra de la empresa. Esta política indica que la gerencia de Seguridad Informática toma las decisiones respecto de los nuevos tipos de privilegios, mientras que ciertas organizaciones pudieran utilizar a los Propietarios de la información para ello. Igualmente, esta política informa de manera indirecta a los usuarios que no deben tratar de descubrir privilegios que no estén expresamente autorizados a utilizar.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#)” y “[Dependencia de Mecanismos Comunes para los Controles](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

33. Sistemas de Seguridad Independientes

Política: La seguridad de un sistema de computadores jamás debe depender totalmente de la seguridad de otro sistema de computadores.

Comentario: En una red de sistemas bien asegurada, cada sistema puede mantener su propia seguridad de manera descentralizada, ya que se proporciona una mayor resistencia ante distintos ataques. Por ejemplo, si un pequeño sistema dependiese totalmente de otro sistema en una red, el quebrantamiento exitoso de la seguridad del otro sistema dejaría vulnerables a ambos. Esto podría suceder si se emplearan sistemas de acceso único porque la misma contraseña podría permitir el acceso a distintos sistemas. Esta política requiere que los diseñadores y otros integrantes del personal técnico

tomen en consideración si un sistema depende en realidad de otro sistema. La política estimula la presencia de medidas de control que compensen las deficiencias o fallas de otros controles. Un ejemplo de esto sería un sistema de ingreso activo que pudiera eliminar el identificador de un usuario porque la actividad que se desarrolla con ese identificador es muy distinta de la del perfil del usuario autorizado.

Políticas Relacionadas: “[Pericia en Sistemas](#),” “[Autentificación del Usuario por el Sistema Operativo](#),” y “[Dependencia de Mecanismos Comunes para los Controles](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

34. Otorgamiento de Acceso a la Información de la Organización

Política: El acceso a la información de la Empresa X siempre debe estar autorizado por el Propietario designado de dicha información, y debe limitarse a aquellas personas que lo necesiten.

Comentario: Esta política indica quién toma las decisiones respecto del acceso a cierta información. La política permite a los Propietarios crear categorías de usuarios, tales como analistas de cuentas por pagar, a las cuales se puede conceder luego un conjunto predeterminado de privilegios. Esto permite a los Custodios conceder privilegios básicos a una persona, basándose en su puesto de trabajo, lo cual hace innecesario tomar en cuenta las circunstancias de cada persona. Asimismo, la política recuerda a todos los lectores que el acceso a la información no se concede simplemente porque fue solicitado, sino que hace falta también la necesidad de tal acceso. Unas cuantas empresas están sustituyendo la noción tradicional de ‘necesitar conocer’ por la noción de ‘necesitar retener’.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#),” “[Control de Acceso a Computadores de Red](#),” y “[Mal Funcionamiento del Control de Acceso](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9.02 Administración del Acceso de Usuario

9.02.01 Registro de Usuarios

1. Identificadores de Usuarios Anónimos

Política: Los identificadores de usuario deben ser asignados en secuencia numérica, de modo que no exista una correlación evidente entre el identificador de usuario y su nombre.

Comentario: Esta política evita que personas no autorizadas puedan emplear identificadores de usuario para irrumpir en los sistemas, deducir información confidencial, o en su defecto, comprometer la seguridad del sistema. Por ejemplo, esto podría suceder si un espía industrial entrase al archivo de papelera y recuperara una libreta telefónica y, además, un registro de actividades del sistema. Si los identificadores de usuario fuesen equivalentes a los apellidos, el espía podría determinar qué actividades realizaron cuáles usuarios. Entonces, puede recabar información personal sobre ellos, utilizándola para adivinar su contraseña y luego decidir a quién sobornar para que realice ciertas acciones en su nombre. Esta política evita que personas no autorizadas adivinen el identificador de usuario, pero, por desgracia, hace que el correo electrónico y ciertas actividades del sistema se tornen más difíciles y menos amigables. Es posible que el sistema incluya una utilidad de conversión que permita a los usuarios remitir los correos electrónicos a un nombre específico en lugar de al identificador de usuario. No obstante lo anterior, no es obligatorio utilizar el enfoque de "secuencia numérica" para la asignación de identificaciones, si se emplea algún otro procedimiento para ocultar la identidad real de los usuarios. Esta política está diseñada para ambientes de alta seguridad.

Políticas Relacionadas: “[Longitud Mínima de Contraseñas](#)” y “[Norma de Creación para Identificadores de Usuario](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

2. Identificador de Usuario No Anónimo

Política: Todos los identificadores de usuario de los computadores y redes de la Empresa X deben construirse de conformidad con la norma de construcción de identificadores de usuario de la Empresa X, deben indicar claramente el nombre de la persona encargada y, en ninguna circunstancia, deben tales

identificadores de usuario permitirse ser genéricos, descriptivos de un puesto o papel organizacional, descriptivos de un proyecto o anónimos.

Comentario: Esta política exige que los administradores de sistemas, administradores de seguridad y otros que asignen los identificadores de usuario sigan un formato normalizado de construcción para los mismos. Igualmente, esta política evita que los usuarios utilicen seudónimos, bien sea artísticos o de otra clase, porque dichos identificadores anónimos pueden servir para ocultar la identidad de los sujetos que cometan delitos informáticos o, por lo menos, dificultan considerablemente el rastreo de las actividades abusivas o ilegales de una persona específica.

Políticas Relacionadas: “[Identidad del Recolector de Información Privada](#)” e “[Identidad en Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Identificador Unico de Usuario y Contraseña Obligatorios

Política: Todo usuario debe tener un identificador único y una contraseña personal secreta para acceder a los computadores multiusuario y las redes de la Empresa X.

Comentario: Esta política facilita las actividades de administración de la seguridad. Con el constante aumento de la cantidad de computadores y redes en las empresas se complica en demasía la utilización de diversos identificadores de usuario para la misma persona. Por ello, la política lo simplifica tanto para los usuarios como para los administradores del sistema. Otra intención que tiene la política es garantizar que los sistemas multiusuario y las redes tengan software de control del acceso que pueda identificar de manera única y restringir los privilegios de cada usuario. Estas facilidades de control de acceso permiten también el uso de un programa especial para acceder y supervisar el sistema. Para limitar aún más el uso de los computadores por parte de personas no autorizadas, ciertas organizaciones pueden prohibir a los usuarios que empleen la misma contraseña fija en cada computador que usen, aunque pueden utilizar el mismo identificador de usuario. Adicionalmente, lo ideal es utilizar el mismo identificador de usuario en todos los computadores y redes a lo largo de toda la empresa, ya que facilita

considerablemente el análisis de los registros de actividades. Antes de emitir una política como ésta, la organización querrá investigar los nuevos paquetes de administración de seguridad, a menudo conocidos como herramientas de administración de seguridad empresarial. Estas herramientas proporcionan un interface administrativo consistente e independiente de plataforma para los sistemas de control de acceso. El uso que se hace en esta política del término "computador multiusuario" efectivamente exime los terminales de estaciones de trabajo, los computadores personales y demás sistemas pequeños. En muchas organizaciones, estos pequeños sistemas se encargan cada vez más de realizar funciones importantes de producción y de funciones críticas. Si éste es el caso en la organización, hay méritos para eliminar la palabra "multiusuario" de esta política. La política que se describe en esta sección prohíbe igualmente los identificadores de usuario grupales. Ciertas organizaciones querrán sustituir el término "contraseña" por un término más general como "autenticación positiva del usuario", lo cual permitiría el uso de tarjetas inteligentes, tarjetas de contraseñas dinámicas, biometría y otras tecnologías.

Políticas Relacionadas: "Acceso a la Información Secreta," "Identificadores de Usuarios Anónimos," "Identificadores de Usuarios Únicos," "Contraseñas de Control de Acceso al Sistema," y "Contraseñas en Distintos Sistemas"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Vencimiento de los Identificadores de Usuario para No Empleados

Política: Todo identificador de usuario establecido para un no empleado debe tener una fecha de vencimiento especificada, con vencimiento predeterminado de 30 días cuando no se conozca su vencimiento.

Comentario: Esta política garantiza que los identificadores de usuario empleados por externos no continuarán activados tiempo después de que estos individuos hayan cesado su relación laboral con la Empresa X. Sin una fecha de vencimiento, muchos de estos identificadores de usuario permanecerán activos por largos períodos de tiempo, especialmente en aquellas organizaciones donde no existe o es informal el proceso de notificación acerca de las salidas de terceros. Al finiquitar estos identificadores de usuario rápidamente, se reduce el riesgo de uso no autorizado, espionaje industrial, sabotaje y otros abusos. Esta política también ayudará a mantener rápidos tiempos de respuesta y bajos requerimientos de

espacio en disco. Nada de especial tiene el período de 30 días mencionado. Igualmente puede ser cualquier otro período de tiempo.

Políticas Relacionadas: "Privilegios de Identificadores de Usuarios Inactivos" y "Manejo de Despidos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Finiquito de los Privilegios de Acceso

Política: Todos los privilegios informáticos proporcionados por la Empresa X deben terminar cuando el trabajador cesa sus servicios a la misma.

Comentario: Esta política gira instrucciones a los administradores de sistemas, de redes y demás cargos similares en el sentido de revocar con prontitud los privilegios de los empleados que ya no trabajen para la Empresa X. A menudo, se ignoran estos asuntos administrativos por atender otros asuntos más inmediatos. En algunos casos, se mantienen los privilegios del sistema como cortesía hacia un empleado que no tenga acceso a correo electrónico o Internet. Cualquiera que sea la razón, si no se eliminan los privilegios con prontitud, los ex-empleados podrían cometer acciones de sabotaje, espionaje industrial y otras. Ciertas organizaciones desearían moderar esta política, permitiendo el envío de correos electrónicos por cierto tiempo después de la salida del empleado de la Empresa X. Esta política estimula el desarrollo de un sistema interno que comunique los cambios ocurridos en las condiciones laborales del trabajador a los administradores del sistema y a otros encargados de alterar los privilegios en el sistema.

Políticas Relacionadas: "Informe de Cambios en Situación de Empleados"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Vencimiento de los Identificadores de Usuario

Política: Deben establecerse fechas de vencimiento para todos los identificadores de usuario almacenados en los sistemas multiusuario de la Empresa X, después de las cuales dichos identificadores quedarán inhabilitados. Los archivos correspondientes quedarán retenidos durante las siguientes dos semanas.

Comentario: Esta política define el enfoque de la organización para autorizar y otorgar privilegios en el sistema, el cual resulta particularmente importante para una universidad o cualquier otra organización que cuente con personas con relaciones relativamente estables. Otras organizaciones pueden hacer uso de esta política, incluso no teniendo relaciones concretamente definidas. Esta política revoca automáticamente los privilegios relacionados con los identificadores de usuarios inactivos, de modo que no puedan ser utilizados por hackers u otros no autorizados. Asimismo, la política exige a la administración que examine periódicamente los privilegios asignados a cada usuario y determine si deben renovarse o quizás sólo modificarse. Esta política está redactada de tal modo que los administradores de sistemas puedan definir distintos plazos para diferentes usuarios. La referencia al período de dos semanas de retención de los archivos informa a los usuarios que necesitan hacer sus respaldos para que preserven sus datos después de terminar su relación con la empresa. La cláusula de las dos semanas también ayuda a preservar el espacio en disco.

Políticas Relacionadas: “[Vencimiento de Identificador de Usuario](#)” y “[Reautorización de los Privilegios de Acceso de Usuario](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Identificadores de Usuarios Unicos

Política: Todo identificador de usuario en un computador y sistema de comunicación debe identificar de un modo particular a un solo usuario y no deben crearse o utilizarse identificadores de usuario grupales.

Comentario: Esta política establece una conexión definitiva entre el identificador de usuario y una persona. Sin identificadores únicos de un solo usuario, un solo proceso o un solo sistema, los registros resultarían ambiguos y serían considerablemente menos útiles durante las investigaciones para resolver problemas. Dicha ambigüedad puede evitar la toma de acciones disciplinarias o la participación en un juicio por abusos informáticos. También evitara suministrar el adiestramiento correctivo necesario. Sin identificadores de usuario únicos, no se pueden restringir los privilegios individuales. Si los privilegios no se pueden restringir por usuario, resultará difícil implementar una separación de tareas, un control dual, un acceso a la información con base en la necesidad de conocerla y otras medidas de seguridad generalmente aceptadas. Esta es una

política fundamental que sustenta muchas de las políticas y procedimientos de control de acceso. Ciertas organizaciones querrán extender las palabras “identificar de manera única a un solo usuario”. Nada de lo incluido en esta política evita la instalación de sistemas que hagan a los computadores específicos involucrados transparentes al usuario. Por ejemplo, los usuarios pueden registrarse en una aplicación con base en la red y no en un sistema de computadores específico.

Políticas Relacionadas: “[Identificador Unico de Usuario y Contraseña Obligatorios](#)” y “[Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Identificadores de Usuario Genéricos

Política: Los identificadores de usuario deben identificar de manera única a individuos específicos y no deben crearse o utilizarse identificadores genéricos basados en cargos o tareas.

Comentario: Esta política evita que los administradores de sistemas y demás integrantes del personal técnico creen identificadores genéricos basados en los cargos desempeñados. Este es un atajo que utilizan muchos integrantes del personal técnico para disminuir los gastos generales relacionados con los cambios en las condiciones de trabajo de un trabajador. Con este atajo, simplemente, se puede cambiar la contraseña relacionada con el identificador de usuario. La nueva persona que cumple ese rol utilizaría una nueva contraseña, en tanto que la persona saliente tan sólo conocería su antigua contraseña. Si bien esta propuesta parece apetecible en teoría, en realidad pueden surgir dificultades al momento de leer los registros del sistema. Por ejemplo, si se han alterado los relojes del sistema, puede que resulte difícil determinar cuál persona estuvo utilizando cuál identificador genérico. Más preocupante aún es el procedimiento en el cual se asignan identificadores genéricos y se utilizan contraseñas compartidas cuando, por circunstancias, ciertas personas tienen el mismo cargo. En dicho ambiente se hace muy difícil, si no imposible, lograr establecer la responsabilidad del usuario individual sólo a través de los registros. Otra de las razones por las que se puede seleccionar la propuesta del identificador genérico tiene que ver con los sistemas de administración de bases de datos y la delegación de privilegios. Esta misma idea se aplica a los privilegios que se pueden incorporar a los objetos o programas especiales. En cualquiera de las dos instancias, se utiliza el concepto de herencia de privilegios, lo cual quiere

decir que la eliminación de un usuario puede ocasionar problemas en cascada con otros usuarios o procesos. Por ello, antes de adoptar esta política, la organización debe investigar las implicaciones para con los programadores internos y demás integrantes del personal técnico. Además, no es aconsejable el uso de identificadores genéricos porque no permite la simple existencia de archivos dentro de los directorios del empleado saliente sin modificación alguna, hasta que las reclamen, archiven o borren. Esta política está redactada de tal modo que no se puedan asignar identificadores de usuario grupales para contratistas, empresas proveedoras de servicios y otros terceros.

Políticas Relacionadas: “Identificador Único de Usuario y Contraseña Obligatorios” y “Contraseñas de Control de Acceso al Sistema”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Re-Utilización de Identificadores de Usuario

Política: Todo identificador de usuario dentro del sistema de computadores y de comunicaciones de la Empresa X debe ser único, debe estar relacionado solamente con el usuario al cual se asignó y no debe ser reasignado luego de terminar la relación del empleado o cliente con la Empresa X.

Comentario: Esta política elimina la confusión en torno a la identificación real de un usuario en aquellos casos en los que uno o más usuarios reciben un identificador que había sido asignado a otro. Con esta política, los registros serán más confiables y se facilitará la realización de investigaciones forenses. Si la implementación de esta política en determinadas empresas pareciera demasiado compleja, un paso útil en esta dirección sería la imposición de un período prolongado de espera, por ejemplo de un año, antes de reasignar el identificador de usuario ya utilizado. Esta política facilita la aceptación de empleados salientes que luego son reenganchados. Los identificadores de usuario pueden recibir otras denominaciones, tales como cuentas, nombres del usuario o nombres artísticos, pero la idea que está detrás de la política es la misma.

Políticas Relacionadas: “Privilegios de Identificadores de Usuarios Inactivos” e “Identificadores de Usuarios Anónimos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Norma de Creación para Identificadores de Usuario

Política: Los identificadores de usuario de un trabajador de la Empresa X deben ser iguales en cada sistema de computación y deben cumplir las normas para el nombramiento de identificadores de usuario establecidas por el departamento de Tecnología Informática.

Comentario: Esta política simplifica la labor administrativa y de seguridad de los sistemas de computación conectados en red. En muchas organizaciones, el hecho de asignar diversos identificadores de usuario a una sola persona puede generar gran confusión, lo cual resulta particularmente poco deseable en el momento en que el trabajador deja de trabajar en la empresa, porque el personal podría enredarse al tratar de determinar cuál de los identificadores de usuario debe ser desactivado. Esta política simplifica estas actividades, entre ellas actividades criminalísticas, tales como el análisis de los registros a raíz de la investigación de un delito informático. En algunos casos, puede resultar imposible llegar a un enfoque consistente para la creación de identificadores de usuario, especialmente si la tecnología no lo permite. Por lo tanto, es imperativo que el procedimiento de creación de los identificadores de usuario que adopte la organización sea lo suficientemente flexible como para satisfacer las distintas limitaciones del sistema operativo o subsistema de seguridad de cada plataforma. La política da un sólido apoyo a las normas centralizadas de nombramiento de identificador de usuario, aunque políticamente hablando, esto se hace difícil de lograr en ciertos ambientes de computación. Además, la política puede resultar costosa, especialmente si una cantidad significativa de sistemas de computación ya se encuentran funcionando con identificadores de usuario no normalizados. La empresa debe realizar un breve análisis de beneficios antes de adoptar esta política, lo cual facilitará el establecimiento y administración de un sistema único de acceso al sistema.

Políticas Relacionadas: “Mecanismo Único de Acceso,” “Identificador Único de Usuario y Contraseña Obligatorios,” “Base de Datos Maestra de Identificadores de Usuario,” e “Identificadores de Usuarios Anónimos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Múltiples Identificadores de Usuario

Política: Todos los empleados de la Empresa X deben utilizar por lo menos dos conjuntos distintos de identificadores de usuarios para dos tipos distintos de computadores, aquéllos conectados a Internet y aquéllos conectados a una red interna.

Comentario: Esta política evita que los hackers y demás intrusos exploten un procedimiento común de ahorro de tiempo de muchos usuarios, que consiste en la selección del mismo identificador de usuario y contraseña en varios computadores. Si los usuarios emplean este enfoque y si los hackers irrumpen en una de las cuentas del usuario, entonces, a los hackers se les facilitará la entrada a otro computador al cual tengan acceso autorizado estos mismos usuarios. Esta política dificulta un poco la vida de los usuarios, pero tiene una justificación sencilla: los computadores independientes serán tratados como un sistema interno conectado a la red. Esta política se recomienda particularmente para aquellas organizaciones que cuentan con sólidas separaciones entre la red interna e Internet.

Políticas Relacionadas: “[Norma de Creación para Identificadores de Usuario](#)” e “[Identificador Único de Usuario y Contraseña Obligatorios](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Autorización de Solicitud de Acceso al Sistema

Política: Todas las solicitudes de privilegios adicionales en los sistemas multiusuario o redes de la Empresa X deben ser presentadas mediante una planilla de solicitud de acceso al sistema debidamente llenada y autorizada por el jefe inmediato del usuario.

Comentario: Esta política garantiza la existencia de la documentación de los cambios en los privilegios del usuario. Dicha documentación será de gran utilidad para los auditores, al momento de determinar si los privilegios de sistema fueron otorgados de conformidad con las instrucciones de la gerencia. Dicha documentación puede también tener importancia al momento de demostrar que el usuario firmó una declaración en la que indica que estos privilegios eran exigencia del empleo. Esta declaración puede servir de gran utilidad en acciones disciplinarias o juicios. Para los efectos de su implantación, lo deseable es girar instrucciones a la gerencia respecto del proceso de autorización, de modo que no procedan a firmar las solicitudes sin antes determinar si son necesarios los privilegios solicitados.

La implantación podría incluir también la verificación de la firma del gerente con una firma archivada. Los sistemas monousuario están exentos de esta política, debido a que la mayoría se encuentra a menudo bajo el control exclusivo de un solo usuario. Esta política podría modificarse fácilmente, de modo que se podría implementar utilizando planillas electrónicas conjuntamente con firmas y certificados digitales.

Políticas Relacionadas: “[Formularios para Identificadores de Usuario](#)” y “[Otorgamiento de Acceso a la Información de la Organización](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

13. Privilegios de Identificadores de Usuarios Inactivos

Política: Despues de 30 días de inactividad, deben revocarse automáticamente todos los privilegios de los identificadores de usuario.

Comentario: Los identificadores o cuentas inactivos de un usuario han sido utilizados por muchos para cometer fraude y sabotaje. Los usuarios no autorizados consideran que estos identificadores inactivos son atractivos, ya que es poco probable que los usuarios autorizados observen alguna actividad no autorizada. Esta política elimina la oportunidad que tendrían los usuarios no autorizados de emplear identificadores inactivos para fines no autorizados. Asimismo, esta política limpia los registros de control del acceso, de modo que reflejen únicamente los privilegios respectivos de los usuarios activos. No hay nada de especial en el período de 30 días que se menciona en esta política; porque podría haber sido cualquier otro plazo. Si un usuario autorizado sale de vacaciones o de permiso no remunerado por un período extendido, esta política daría como resultado la revocatoria de su identificador de usuario. A su regreso, el usuario podría solicitar al administrador de seguridad la devolución de sus privilegios. Luego, el administrador verificaría la condición de la persona y otorgaría la solicitud, si procede. El identificador de usuario involucrado puede seguir definiéndose, aun cuando se hayan revocado los privilegios relacionados con éste. Además, los archivos pertenecientes al usuario pueden seguir en el disco, pese a que ya le han sido revocados los privilegios. Debido al hecho de que los administradores de sistemas se encuentran a menudo muy atareados, puede que no encuentren tiempo para revocar los privilegios de los usuarios a tiempo. Por ello, la versión automatizada de esta política actúa como una malla de seguridad que reduce las

vulnerabilidades producidas por la falta de atención a este asunto por parte del administrador. Otra de las razones por la que se deben revocar, pero definir, los identificadores de usuario en forma temporal es que brinda al administrador correspondiente la oportunidad de revisar los archivos relacionados con el identificador de usuario y, posteriormente, desechar o transferir la responsabilidad de estos archivos, según corresponda. Esta política se aplica a los correos de voz y a otros sistemas, además de los sistemas multiusuario de uso general. Ciertas organizaciones revocan los privilegios de las personas ajenas a la empresa, tales como contratistas, asesores, empleados temporales y clientes luego de un breve período de tiempo de inactividad, pero proporcionan un período de tiempo más prolongado para los empleados.

Políticas Relacionadas: “[Última Hora y Fecha de Inicio de Sesión](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

14. Formularios para Identificadores de Usuario

Política: Los usuarios deben firmar tanto un acuerdo de confidencialidad como un convenio de seguridad del sistema informático antes de emitírseles el identificador de usuario que les permita acceder a los sistemas de la Empresa X.

Comentario: Antes de obtener el acceso a cualquier sistema de la Empresa X, los usuarios deben recibir información sobre las políticas de seguridad y sus responsabilidades inherentes. La idea fundamental de esta política es no otorgar el identificador hasta que los usuarios hayan acordado, por escrito, respetar los reglamentos básicos que rigen el uso del sistema. Si los usuarios no firman estos acuerdos al momento de obtener su identificador de usuario, será difícil lograr que los firmen después. Igualmente, estos acuerdos pueden ser importantes en juicios y acciones disciplinarias. El papeleo para emitir el identificador de usuario puede incluir los acuerdos mencionados en la política u otros acuerdos, dependiendo de las necesidades de la organización.

Políticas Relacionadas: “[Convenio de Cumplimiento](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

15. Informe de Cambios en Situación de Empleados

Política: La gerencia debe informar con prontitud todos los cambios significativos ocurridos en las tareas y condiciones laborales de los usuarios finales a los administradores de seguridad que manejen sus identificadores de usuario.

Comentario: Los privilegios de los usuarios finales deben quedar suspendidos con prontitud, en el caso de que la persona haya sido despedida, transferida, ascendida, dada de permiso sin remuneración o, de algún otro modo, ya no desempeñe el mismo cargo. Por lo general, los administradores de seguridad de sistemas desconocen estos cambios, a menos que reciban una notificación del gerente correspondiente o del departamento de Recursos Humanos. Se recomienda una política separada, pero parecida, que requiera mantener la información relativa a los cambios laborales en estricta privacidad, ya que el empleado finiquitado podría entablar una demanda legal por difamación. Esta política podrá utilizarse cuando se necesite establecer procedimientos normalizados que notifiquen a los administradores de cambios en las condiciones laborales del empleado. En las empresas más sofisticadas, se transmite un aviso automático por correo electrónico desde la base de datos del departamento de Recursos Humanos hasta los administradores de seguridad.

Políticas Relacionadas: “[Acceso Físico de Trabajadores Cesados](#)” y “[Transferencia de Responsabilidad en Custodia](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

16. Cambios en Situación de Usuarios

Política: Todo usuario debe notificar a la Unidad de Administración de Sistemas de los cambios en su relación con la Empresa X.

Comentario: Esta política informa a los usuarios que deben reportar a los administradores de sistemas de la Empresa X los cambios en su relación con la compañía. Esta política no evita que los administradores de sistemas obtengan, al mismo tiempo, notificaciones del departamento de Recursos Humanos sobre cambios en las condiciones del usuario, o de los jefes del usuario. Es poco probable que los propios usuarios reporten ciertos cambios, tales como los despidos y, por lo tanto, deben venir de otras fuentes. También, lo ideal es la alimentación desde múltiples fuentes hacia la unidad de administración de sistemas ya que, en ocasiones,

algunas no distribuyen la información. Las fuentes múltiples de información sobre cambios en las condiciones laborales del empleado permiten también que los administradores del sistema corroboren solicitudes poco usuales antes de actuar en consecuencia. Asimismo, la política proporciona a los administradores del sistema la información necesaria para comunicarse de inmediato con los usuarios y preguntarles si ellos, o algún intruso que utilice las mismas cuentas, han iniciado alguna actividad que implique abuso.

Políticas Relacionadas: “[Cambios en Situación del Trabajador](#)” e “[Informe de Cambios en Situación de Empleados](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Transferencia de Responsabilidad en Custodia

Política: En el momento en que un trabajador deja su cargo en la Empresa X, su jefe inmediato debe revisar con prontitud los archivos y documentos guardados en el computador, con el fin de reasignar las tareas y delegar específicamente la responsabilidad de estos archivos que anteriormente estaban en manos del ex-trabajador.

Comentario: La intención de esta política es transferir al custodio las responsabilidades de manera clara y expedita, garantizando así que se mantienen las medidas de seguridad mínimas. Es de especial importancia el proceso de reasignación de tareas, en caso de que los archivos contengan información sensible, crítica o valiosa. Igualmente, esta política informa a los empleados que otras personas examinarán sus archivos después de abandonar la empresa. Con esta política, se notifica a la gerencia de la responsabilidad de manejar adecuadamente la información del empleado saliente y se evita cualquier fraude, sabotaje y demás abusos que con frecuencia se llevan a cabo cuando no hay ninguna persona encargada de cierta área.

Políticas Relacionadas: “[Acceso Físico de Trabajadores Cesados](#)” y “[Propiedad de la Información](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

18. Eliminación de Archivos de Trabajador Cesado

Política: Salvo que el departamento de Operaciones Computarizadas haya recibido instrucciones al contrario, se deben depurar todos los archivos residentes en los directorios del usuario, cuatro semanas después de la salida permanente del empleado de la Empresa X.

Comentario: Esta política fija una fecha para la eliminación automática de los archivos guardados en los directorios específicos del usuario. La existencia de una fecha límite específica obligará a la administración encargada de los empleados cesados a examinar dichos archivos y reasignarlos a otros empleados. Esta política puede utilizarse también para notificar a los usuarios sobre la necesidad de respaldar sus propios datos, especialmente en aquellos ambientes en los que se producen cambios importantes de usuarios, tal como ocurre con los computadores multiusuario destinados a estudiantes universitarios. Las palabras “salida permanente” son utilizadas para evitar la eliminación de archivos si el trabajador toma un permiso, un año sabático, sale de permiso prenatal, o tiene alguna otra ausencia extensa pero temporal. Esta política también sirve para preservar el espacio en disco y, además, puede utilizarse para disminuir el trabajo manual de administración, si viene acompañada de un subprograma que logre estos objetivos de forma automática. Para mayor seguridad, los archivos pueden guardarse en una cinta de respaldo mientras no necesiten borrarse con nueva información. Esta política supone que ya funciona un proceso para enterar a los gerentes de sistemas sobre las salidas de los trabajadores. Asimismo, esta política supone que los gerentes son capaces de identificar de inmediato los sistemas en los cuales los empleados salientes tenían identificadores de usuario. Se recomienda al departamento de Operaciones Computarizadas notificar a la administración que los archivos del empleado saliente serán eliminados a partir de una fecha determinada, a fin de lograr que asuman esta política con la debida seriedad. Las palabras “Operaciones Computarizadas” podrían cambiarse por “Administración de Sistemas” u otra designación funcional.

Políticas Relacionadas: “[Base de Datos Maestra de Identificadores de Usuario](#)” y “[Transferencia de Responsabilidad en Custodia](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

19. Vencimiento de Identificador de Usuario

Política: Se debe fijar a seis meses el vencimiento de los identificadores de usuario residentes en los computadores accesibles desde internet, contados a partir del momento de su establecimiento, con renovación cada seis meses.

Comentario: Esta política desestimula y limita la utilización de identificadores de usuario en computadores accesibles desde internet porque los intrusos podrían explotarlas, por lo que resulta conveniente mantenerlas a niveles mínimos. La renovación periódica de dichos identificadores representa sólo un inconveniente menor. Lo más importante de todo es que el requisito que se describe en esta política echa por tierra una posible vía de comprometer el sistema involucrado si el identificador de usuario ya no está activo. La mayor parte de las actividades en internet se puede realizar a través de computadores protegidos por cortafuegos. Asimismo, en algunos casos, se hará necesario informar a los usuarios que no necesitan un identificador para trabajar en un computador accesible desde internet para poder enviar correos electrónicos. Normalmente, cualquier servidor de correo de una red interna podrá también enviar y recibir correos electrónicos a través de Internet. Ciertas organizaciones hacen pasar momentos difíciles a los usuarios, al exigirles identificación en un computador accesible desde internet. Los usuarios pueden solicitar estos identificadores, debido a que proporcionan una forma más sencilla de realizar varias tareas que también pueden lograrse con sistemas

internos que cuenten con mejor protección. No tiene nada de especial el período de seis meses, ya que podría ser igualmente de tres meses.

Políticas Relacionadas: “[Contraseñas Iniciales](#)” y “[Vencimiento de los Identificadores de Usuario](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

20. Autentificación para Cuentas Nuevas

Política: Cada vez que la Empresa X abra una nueva cuenta con un cliente, debe autenticar la identidad del cliente de manera definitiva.

Comentario: Esta política evita que los perpetradores de fraude o de robo de identidad utilicen el anonimato que brindan Internet, el teléfono y otros sistemas remotos de comunicación como excusa para no proporcionar una identificación definitiva. Obtener una identificación robusta no es difícil y se puede lograr a través del suministro de un cheque invalidado. Este enfoque se utiliza ampliamente en la industria bancaria para autorizar los pagos automáticos en las cámaras de compensación. Esta política es deliberadamente vaga en lo relativo a la apertura de cuentas de manera remota o en persona.

Políticas Relacionadas: “[Acceso a la Información Personal](#)” y “[Validación de la Identidad de Terceros](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

9.02.02 Administración de Privilegios

1. Restricción de Privilegios — Necesidad de Conocer

Política: Los privilegios en sistemas de computación y de comunicaciones de todos los usuarios, sistemas y programas deben restringirse de acuerdo con la necesidad de conocer.

Comentario: Esta política previene el otorgamiento de privilegios excesivos a los usuarios, porque a menudo permiten que realicen acciones abusivas o no autorizadas, tales como visualizar información privada ajena. Los privilegios excesivos también pueden hacer que los usuarios cometan errores con serias consecuencias, como por ejemplo tumbar un servidor de comunicaciones durante horas hábiles. Este enfoque

mejora notablemente con un esquema de clasificación de datos. La política podría redactarse de manera de enfatizar la información versus los sistemas. El acceso a la información se otorgaría cuando exista la necesidad de conocer. Igualmente, el término “necesidad de conocer” podría ser reemplazado con terminología más general, tales como “necesidad legítima de negocios” o “necesidad demostrable de negocios.”

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#),” “[Privilegios Especiales en Sistema](#),” “[Otorgamiento de Acceso a la Información de la Organización](#),” “[Naturaleza y Ubicación de la Información de la Organización](#),” “[Restricción de Privilegios — Necesidad de Retener](#),” y “[Acceso a Información Sensible o Valiosa](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

2. Restricción de Privilegios — Necesidad de Retener

Política: El acceso a los sistemas de computación y de comunicaciones de la Empresa X debe ser otorgado a todos los empleados, a menos que la gerencia a cargo de un sistema específico haya definido reglas específicas de control de acceso.

Comentario: Esta política otorga a todos los empleados acceso a los recursos internos del sistema, lo cual debe estimularlos y motivarlos para desempeñar mejor su trabajo. Los expertos lo denominan administración a libro abierto, en lugar de llamarlo necesidad de retener información para controlar el acceso. Este enfoque ha sido anunciado como una manera de facilitar flujos de información más rápidos y más eficientes dentro de una empresa e incluso ciertas compañías progresivas lo han adoptado. En el enfoque tipo retención, la responsabilidad pasa desde los usuarios, que deben demostrar su necesidad de acceso, tal como ocurre en el enfoque tradicional, hacia la administración, que debe demostrar su necesidad de restringir el acceso. A manera de balance, algunos expertos en seguridad informática defienden el uso de la necesidad de conocer cuando se trata de información confidencial, y el de la necesidad de retener cuando se trata de información no confidencial. El enfoque ‘necesaría retener’ resulta menos costoso que el enfoque ‘necesitar conocer’, debido a que se puede implementar con menos decisiones respecto de los permisos de acceso. Aunque aparente ser más atractivo, el enfoque ‘necesaría retener’ puede colocar a los sistemas informáticos internos en condición vulnerable y peligrosamente abierta. En esta política no se mencionan contratistas, trabajadores temporales ni consultores.

Políticas Relacionadas:“Restricción de Privilegios — Necesidad de Conocer,” “Naturaleza y Ubicación de la Información de la Organización,” y “Acceso a Información Sensible o Valiosa”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

3. Usuarios Especiales Privilegiados

Política: Todos los sistemas de redes y de computadores multiusuario deben soportar un tipo especial de identificador de usuario que cuente con privilegios

ampliamente definidos que habiliten a personas autorizadas para modificar la condición de seguridad del sistema.

Comentario: Esta política requiere que la gerencia establezca un tipo especial de identificador de usuario con mayores privilegios que el identificador de usuario normal. Dicho identificador de usuario con mayores privilegios podría, por ejemplo, hacer respaldos de todos los datos en un disco del sistema, tumbar el sistema o dar por terminada la sesión de otro usuario. Asimismo, hay que cambiar la condición de seguridad del sistema cuando se asignan identificadores a nuevos usuarios y cuando se instala una nueva versión del sistema operativo. Al tener un tipo separado de usuario privilegiado para estas tareas especiales, la administración evita dar privilegios tipo ‘super’ usuario a todos los usuarios. No es sólo posible sino deseable, por razones de respaldo del personal, que exista más de un usuario privilegiado para cada sistema.

Políticas Relacionadas:“Privilegios Predeterminados de Usuario”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

4. Privilegios Especiales en Sistema

Política: Los privilegios especiales en sistemas, tales como la capacidad para examinar los archivos de otros usuarios, deben limitarse a aquellos que están encargados directamente de la administración o seguridad de los sistemas, y sólo deben otorgarse a aquéllos que hayan asistido a una sesión autorizada de adiestramiento como administrador de sistemas.

Comentario: Esta política limita los privilegios especiales en sistemas, tales como la capacidad para reiniciar el servidor de red de área local, a aquellas personas que verdaderamente necesitan estos privilegios para realizar su trabajo. La organización querrá sustituir las palabras “administración o seguridad de los sistemas” por los cargos que estas personas desempeñan en su empresa.

Políticas Relacionadas:“Cantidad de Identificadores de Usuarios Privilegiados” y “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

5. Cantidad de Identificadores de Usuarios Privilegiados

Política: La cantidad de identificadores de usuarios privilegiados debe limitarse estrictamente a aquellas personas que necesariamente deban contar con dichos privilegios por razones autorizadas de negocios.

Comentario: El propósito de esta política es suministrar instrucciones a los administradores de sistemas y de seguridad sobre cómo asignar los identificadores de usuarios privilegiados a los usuarios. Si una cantidad significativa de usuarios poseen identificadores de usuarios privilegiados, resultará difícil, si no imposible, mantener una seguridad adecuada. Esta política implica la existencia de un proceso de aprobación para el otorgamiento de los identificadores de usuarios privilegiados. Algunas organizaciones querrán especificar el proceso de aprobación por parte de la administración, mientras otras limitan la cantidad de identificadores de usuarios privilegiados a una cantidad específica. Por lo general, no se recomienda esta propuesta, ya que puede interferir indebidamente con el desempeño de las actividades empresariales normales. Esta política supone que las palabras "identificador de usuario privilegiado" han sido definidas en alguna parte. Por lo general, estos identificadores de usuario permiten que los usuarios revisen los archivos de otros usuarios, modifiquen el software de los sistemas y ejecuten otros potentes comandos de sistema.

Políticas Relacionadas: "[Privilegios Especiales en Sistema](#)" y "[Acceso a Comandos del Sistema Operativo](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Identificador de Usuario Administrador

Política: Los administradores de sistemas que manejan sistemas de computación con más de un usuario deben tener por lo menos dos identificadores de usuario, uno que le proporcione acceso privilegiado al sistema con su respectivo registro, y otro que le proporcione privilegios de un usuario normal, para efectuar su trabajo diario.

Comentario: Esta política tiene como objetivo separar el trabajo de los administradores de sistemas en dos categorías distintas, cada una de las cuales tienen distintas necesidades de privilegio en el control de acceso. Al segmentar el trabajo que realizan los administradores de sistemas, esta política otorga el acceso con base en la necesidad de conocer. No se utilizan más privilegios de lo necesario para lograr un

objetivo de negocios específico. Los administradores de sistemas saben que sus actividades son registradas y revisadas cuando utilizan identificadores de usuarios privilegiados y eso los estimula a emplearlos en forma sensata y con moderación. Sin una política como ésta, los administradores de sistemas podrían utilizar sus identificadores de usuario privilegiado para realizar actividades que, de otro modo, les estarían prohibidas, restringiéndose entonces a los privilegios de un usuario normal. Los administradores de sistemas podrían no notar estas restricciones, a menos que realmente se utilicen dos o más identificadores de usuario. Asimismo, esta política facilita aún más el análisis de los registros y revisiones, ya que no se incluye gran cantidad de información irrelevante en los registros detallados de las actividades efectuadas con el identificador de usuario privilegiado. Esta política resulta particularmente importante para los empleados que trabajan como administradores de sistemas a medio tiempo.

Políticas Relacionadas: "[Restricción de Privilegios — Necesidad de Conocer](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Autorización de Identificador de Usuario y Privilegio

Política: Los identificadores de usuario, los privilegios de sistemas de aplicaciones de negocios y los privilegios de sistemas que superen las capacidades rutinariamente otorgadas a los usuarios, deben ser autorizados con antelación por, respectivamente, el supervisor inmediato del usuario, el Propietario de la información y el gerente del departamento de Soporte Técnico.

Comentario: Esta política tiene como objetivo definir quién debe autorizar la emisión del identificador de usuario y quién debe autorizar el otorgamiento de los privilegios en las aplicaciones y en los sistemas. Esta política asume que el administrador de sistemas, o un especialista en seguridad de sistemas, llevará a cabo el proceso de otorgar un identificador de usuario y sus privilegios correspondientes. Tal como está redactada, la política no menciona métodos permisibles para comunicar dichas autorizaciones, los cuales normalmente incluyen el correo electrónico, memos internos y conversaciones telefónicas. Ciertas organizaciones podrán requerir métodos de comunicación que creen un rastro definitivo para las auditorías, mientras otras querrán métodos de comunicaciones que no puedan ser burlados con facilidad. En ciertos casos, la autorización

de los privilegios del sistema por parte de la administración debe hacerse por escrito. La política asume que el término "Propietario de la información" ya ha sido definido.

Políticas Relacionadas: "Propiedad de la Información" y "Privilegios Predeterminados de Usuario"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Acceso a Comandos del Sistema Operativo

Política: No se debe permitir que los usuarios finales utilicen comandos a nivel de sistema operativo, mediante su limitación a los menús que muestran sólo aquellas funciones para las cuales han sido autorizados.

Comentario: Esta política restringe de manera significativa el acceso a potentes comandos del sistema, tales como reformatear un disco duro en un servidor de red de área local, lo cual mejora la seguridad del sistema. A menudo, ofrecer únicamente menús resulta más beneficioso para el usuario que permitirle utilizar comandos del sistema operativo. Los menús deben mostrar solamente las opciones que han sido autorizadas para dicho usuario. También se debe prohibir a los usuarios salir de estos menús, mediante el uso de "break", Control-C y otros comandos relacionados. Cuando los usuarios deseen salir del menú del sistema, deben hacerlo terminando su sesión. El software necesario para implementar esta política forma parte de varios sistemas operativos, mientras que otros requieren de un paquete de software separado.

Políticas Relacionadas: "Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema" y "Cantidad de Identificadores de Usuarios Privilegiados"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Actualización de Información de Producción

Política: Los privilegios en sistemas deben definirse de modo tal que el personal no relacionado con el área de producción, incluyendo entre otros a auditores internos, administradores de seguridad informática, programadores y operadores de computadores, no pueda actualizar la información de producción.

Comentario: Las actualizaciones se deben completar únicamente a través de canales normales; por ejemplo, sólo se permiten las actualizaciones de la base de datos de recursos humanos, si son iniciadas por el personal autorizado del departamento de Recursos Humanos. Permitir que otras personas hagan actualizaciones es una invitación a cometer abusos. El personal de soporte técnico debe poder revisar la información sobre la producción empresarial a fin de detectar errores e inconsistencias y realizar actividades similares, pero no deben poder actualizar la información en sí. Esta política podrá requerir de una definición que acompañe la definición del término "producción", particularmente para los usuarios de sistemas pequeños.

Políticas Relacionadas: "Autorización para Transacciones de Producción," "Administrador de Seguridad Designado," y "Modificación de Información por Internet"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Base de Datos Maestra de Identificadores de Usuario

Política: Deben mantenerse registros actualizados que incluyan a todos los sistemas de computación donde los usuarios tengan identificadores de usuario.

Comentario: Esta política garantiza el fácil reconocimiento de todos los identificadores de usuario asignados a un trabajador, así como la rápida revocación de los privilegios correspondientes. Esto será de gran utilidad cuando, por ejemplo, se ha despedido a un empleado con causa justificada, y todos sus identificadores deban desactivarse de inmediato. Incluso, dicha base de datos puede resultar de gran utilidad para determinar a cuáles administradores de seguridad de sistemas debe notificarse cuando se llevan a cabo cambios menos importantes en las condiciones del usuario. Algunas organizaciones incluso mantienen una base de datos centralizada conectada a la base de datos de recursos humanos. Cualquier cambio en la base de datos del departamento de Recursos Humanos provoca la generación automática de mensajes de correo electrónico que se envían a las personas que mantienen la base centralizada. Se podrían enviar los mensajes a los administradores de seguridad de los sistemas o se podría enviar un comando directamente a los sistemas de control de acceso para los que el empleado involucrado tenía un identificador de usuario.

Políticas Relacionadas: “Transferencia de Responsabilidad en Custodia” y “Norma de Creación para Identificadores de Usuario”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Otorgamiento de Privilegios del Sistema

Política: Los privilegios del sistema de computación y del sistema de comunicaciones deben ser otorgados únicamente por una cadena definida de delegación de la autoridad.

Comentario: Esta política define cuáles gerentes pueden otorgar los privilegios de sistema y cuáles son los privilegios específicos que pueden otorgar. Si no existe una cadena definida de delegación, el gerente no tiene la autoridad necesaria para otorgar el acceso a otras personas. Esta noción resulta particularmente importante cuando participan la gerencia departamental y otras gerencias usuarias finales en las actividades de

otorgamiento de los privilegios. Por ejemplo, en el ambiente de una base de datos de un mainframe, los privilegios de acceso se pueden otorgar a otra persona. Al revocarse los privilegios del usuario, su capacidad para delegar privilegios a otros queda también automáticamente revocada, y el software puede implementar esta política de manera automática. Igualmente, esta política apoya la herencia de estos privilegios, que alcanzarán mayor importancia dentro de la programación orientada a objetos (OOP, por sus siglas en inglés). En la OOP, los programas tienen ciertos privilegios que se pueden otorgar a otros programas, pero los privilegios deben seguir una línea clara de delegación del control de acceso.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,” “Acceso a Información Sensible o Valiosa,” “Reportes de Distintivos de Identificación,” y “Lista de Otorgantes de Acceso Físico”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9.02.03 Gestión de Contraseñas de Usuario

1. Contraseñas Iniciales

Política: Las contraseñas emitidas por el administrador de seguridad deben estar vencidas, obligando así al usuario a seleccionar otra contraseña antes de completar el procedimiento de inicio de sesión.

Comentario: El propósito de esta política es garantizar que sólo el usuario final conozca su propia contraseña, lo cual permitirá que la actividad registrada con un identificador de usuario sea atribuida de manera única a ese usuario en particular. El tipo de contraseña inicial mencionado en esta política algunas veces recibe el nombre de contraseña temporal, en el sentido de que tiene validez sólo para una sesión en línea. Ciertos proveedores están haciendo extensiva esta idea a las contraseñas predeterminadas contenidas en sus computadores o en los productos de comunicaciones. Se exige tanto a los administradores como a los usuarios finales cambiar las contraseñas predeterminadas, o iniciales, antes de efectuar cualquier trabajo en el sistema. Esta política asume que no se emplean identificadores de usuario grupales y también que se permite a los usuarios seleccionar sus propias contraseñas.

Políticas Relacionadas: “Estructura de las Contraseñas,” “Contraseñas Proporcionadas por Proveedores,” “Cambios Obligatorios de Contraseña,” y “Códigos de Identificación para Soporte Técnico”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Transmisión de Contraseña Inicial

Política: La contraseña inicial de un nuevo usuario remoto debe enviarse a través de un canal de comunicaciones distinto al canal utilizado para tener acceso a los sistemas de la Empresa X, incluyendo, sin limitantes, el servicio de mensajería que requiera de firma y presentación en persona ante una oficina de un intermediario confiable, conjuntamente con identificación con fotografía.

Comentario: Esta política distribuye de manera segura la contraseña fija inicial, la tarjeta ambulante de identificación o cualquier otro mecanismo de autenticación de la identidad del usuario. En este caso, el principal enfoque de esta política es evitar que sea interceptada por una persona no autorizada. Aun cuando el empleado del servicio de mensajería obtuviese una contraseña fija, le faltaría el identificador de usuario y demás

información sobre la conexión, imposibilitando el uso no autorizado del servicio. La idea detrás de esta política es dividir la información necesaria para ingresar al sistema a lo largo de múltiples canales de comunicación, lo cual dificulta la intercepción de todos ellos. Las reinicializaciones de las contraseñas pueden manejarse remotamente a través del teléfono, siempre que se haya intercambiado anteriormente alguna otra información secreta que se pudiera utilizar para identificar al usuario remoto. Esta política resulta de gran importancia para los teletrabajadores remotos o clientes que utilicen un servicio de alto riesgo por Internet, tal como el de intercambio de acciones bursátiles.

Políticas Relacionadas: “Transmisión de Datos y Claves de Cifrado” y “Envío de Información Sensible”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Confirmación de Cambio de Contraseña Fija

Política: Todos las reinicializaciones o cambios de contraseñas fijas deben confirmarse con prontitud a través de correo regular, de modo que el usuario autorizado pueda rápidamente detectar y reportar cualquier conducta fraudulenta o abusiva.

Comentario: El propósito de esta política es utilizar al usuario como parte de un equipo de seguridad para identificar fraudes y abusos. Muchas organizaciones que soportan comercio por internet utilizan contraseñas fijas y cifrado tipo capas. El problema que presenta este enfoque es que cualquier otra persona puede suministrar ciertos detalles personales por teléfono, y hacerse pasar por el usuario autorizado y solicitar la reinicialización o cambio de la contraseña. Para reducir el daño que puede ocasionar el farsante, la política notifica al usuario autorizado que se cambió la contraseña. Si el sistema no es de alta seguridad, entonces la notificación enviada puede incluir también la nueva contraseña. Igualmente, esta política es importante para el pago de facturas por teléfono y para otros sistemas telefónicos de respuesta automática. Cualquiera que fuese el caso, si el usuario no inicia el proceso de cambio de la contraseña, debería comunicarse con el proveedor del sistema e informar de sus sospechas. Esta misma política puede utilizarse para establecer un nuevo servicio en línea, tales como los procedimientos de reembolso de las ventas de acciones mediante transferencia electrónica que están en manos de una empresa de fondos mutuales. En este caso, el aviso enviado por correo indicaría el establecimiento de las nuevas capacidades en el sistema y pediría al cliente

comunicarse con el proveedor del servicio, si en realidad no lo inició. Para nuevos servicios, las empresas telefónicas de muchas jurisdicciones utilizan la confirmación por correo, sin necesidad de contraseñas. Otra de las razones por la que se envían dichas notificaciones es la reducción de la cantidad de llamadas al departamento de servicios al cliente, pidiendo una contraseña recientemente emitida pero olvidada.

Políticas Relacionadas: “Contraseñas Iniciales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Bajos y medianos

4. Envío de Contraseñas por Correo

Política: En caso de que sean enviadas por correo regular o por sistemas físicos de distribución similares, las contraseñas se deben enviar separadas de los identificadores de usuario, no deben tener marcas que indiquen el origen del envío y deben estar ocultas dentro de un sobre opaco que fácilmente revele si ha sido alterado.

Comentario: Esta política hace más difícil que una persona no autorizada obtenga tanto el identificador de usuario como la contraseña que le permitirían acceso al sistema. El riesgo queda reducido al enviar estos materiales en sobres separados, preferiblemente en horas distintas. Si quedara interceptado sólo uno de los dos sobres, ya no se podría lograr el acceso no autorizado al sistema. Se pueden utilizar sistemas de comunicaciones múltiples; por ejemplo, se puede suministrar el identificador de usuario por teléfono, pero se puede enviar la contraseña por correo. La falta de marcas en el sobre disminuye la posibilidad de que personas no autorizadas presten atención a estos materiales. La última frase de esta política refleja el hecho de que sólo el receptor debe tener conocimiento de la contraseña y que, en caso de que haya sido divulgada durante su recorrido, el usuario debe reportarlo al administrador de seguridad. Es importante usar un sobre opaco, de modo que la persona que maneje el correo no pueda descubrir la contraseña si sostiene el sobre a contraluz. Los ambientes de alta seguridad querrán tomar un paso más en esta separación, segmentando la contraseña en componentes y enviándolos por separado. En este caso, el acceso al sistema se hará posible sólo cuando el usuario reconstruya toda la contraseña y la combine con el identificador de usuario. Esta propuesta de componentes de parámetros secretos se utiliza igualmente en ciertas actividades manuales de gestión de claves de cifrado.

Políticas Relacionadas:“[Sistemas de Gestión de Claves de Cifrado](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

5. Contraseñas Fijas Olvidadas

Política: Todo usuario que olvide o pierda su contraseña debe registrarse nuevamente y recibir nuevo identificador de usuario y nueva contraseña.

Comentario: Esta política evita que un usuario no autorizado se haga pasar por usuario autorizado, utilizando el teléfono para solicitar la reinicialización o cambio de la contraseña y hacer uso de los privilegios del usuario autorizado. Esta política proporciona un enfoque práctico para aquellas organizaciones que no deseen incurrir en costos relacionados con la emisión de una contraseña especial o código secreto que pueda olvidar el usuario. De uso extenso en el campo comercial en Internet, esta política podría resultar adecuada, por ejemplo, para un proveedor de información, tal como ocurre con los servicios por suscripción. Registrarse nuevamente incluiría el suministro de información sobre el número de tarjeta de crédito, nombre, dirección y otros detalles importantes del usuario, y tal vez incluya la creación de un perfil del cliente. Esta política elimina una de las áreas de mayor dificultad para el Centro de Atención al Usuario: la reinicialización y cambio de contraseñas. Igualmente, esta política es ideal debido a que puede automatizarse en su totalidad. Si un cliente no ha tenido ninguna interacción cara a cara o voz a voz con el proveedor del sistema, esta política podría permitir que los clientes sigan utilizando el producto o servicio por su propia cuenta. Esta política podría resultar beneficiosa, cuando los usuarios seleccionan sus propios identificadores de usuario, pero necesitan un nuevo identificador de usuario en vez de utilizar nuevamente el asignado anteriormente. Esta política resulta mejor para los clientes y es menos ideal para usuarios internos, como los empleados de una empresa, que deben tener identificadores de usuario que cumplan con las normas de creación de los mismos. En esta política, la palabra "usuarios" podría sustituirse por "clientes". Al tener los certificados digitales, no se necesita de una política de este tipo, debido a que se da validez automática al identificador de usuario sin emitir nuevamente el identificador y la contraseña. Esta política incrementa la seguridad, a costa de la amigabilidad y facilidad de uso.

Políticas Relacionadas:“[Confirmación de Cambio de Contraseña Fija](#)” y “[Intentos de Introducir Contraseña](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Bajos y medianos

6. Reinicialización de la Contraseña Posterior a la Desactivación

Política: Todos los sistemas de computación de la Empresa X con contraseñas fijas deben estar configurados para permitir sólo tres intentos para introducir la contraseña correcta, luego de lo cual el identificador de usuario debe quedar desactivado, pudiendo reiniciarse solamente a través del personal del Centro de Atención al Usuario cuando el identificador de usuario haya sido autenticado.

Comentario: Esta política evita el acceso no autorizado al sistema mediante la deducción de la contraseña. La propuesta descrita en esta política evita la deducción de una gran cantidad de contraseñas, lo cual podría producirse, por ejemplo, si un sistema UNIX está configurado erróneamente para permitir que personas ajena a la empresa hagan copias del archivo de contraseñas. Esta política informa a los usuarios autorizados que algunas personas han intentado obtener acceso no autorizado a sus identificadores de usuario, porque los mismos quedan desactivados. Este importante control es reflejo de aquellas políticas que exigen a los usuarios crear contraseñas de difícil deducción. El trabajo manual de reinicialización de contraseñas podrían realizarlo personas distintas a las del Centro de Atención al Usuario o lograrse mediante una herramienta administrativa de reinicialización automática de contraseñas; por ejemplo, lo podrían hacer los administradores de sistemas locales o el departamento de Seguridad Informática. Por lo general, no se revocan los privilegios de acceso si se producen introducciones erradas de contraseñas durante un período de tiempo más prolongado. Pese a que esto abre la posibilidad de que un compañero de trabajo trate de deducir la contraseña de otro usuario una o dos veces sin ser detectado, ciertas organizaciones consideran aceptable este pequeño riesgo.

Políticas Relacionadas:“[Transmisión de Contraseña Inicial](#)” y “[Confirmación de Cambio de Contraseña Fija](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

7. Contraseñas en Software

Política: Las contraseñas nunca deben incorporarse al software desarrollado o modificado por los empleados de la Empresa X.

Comentario: Incorporar una contraseña dentro del software significa que la contraseña no se puede modificar con rapidez, lo cual deviene en mecanismos de seguridad inflexibles que no podrían adaptarse rápidamente a nuevas circunstancias. Si los usuarios no introducen contraseñas, lo más recomendable es utilizar las tablas de sistema u otro emplazamiento distinto al software para almacenar las contraseñas. Igualmente se exige el cifrado de las contraseñas. Además de las contraseñas fijas, esta política también es aplicable a otros parámetros de seguridad, tales como claves de cifrado, parámetros para generadores numéricos seudoaleatorios, números de identificación personal y vectores de inicialización.

Políticas Relacionadas: “[Sospecha de Divulgación de Contraseña](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Cambios de Contraseña Luego de Estar Comprometido el Sistema

Política: Si un sistema multiusuario emplea contraseñas fijas como mecanismo primario de control de acceso, todas las contraseñas de dicho sistema deben ser cambiadas de inmediato al comprobarse que el sistema está comprometido, y todos los usuarios deben cambiar sus contraseñas fijas en los demás computadores, si usan esas mismas contraseñas.

Comentario: Esta política podría parecer evidente a los que tienen mucho tiempo trabajando en el campo de la seguridad informática. Sin embargo, no es evidente para los administradores de sistemas, de redes y otros integrantes recientes del personal. Aunque el cambio de las contraseñas fijas no erradique la fuente del compromiso, sí constituye un paso necesario hacia el re establecimiento de un ambiente confiable. Igualmente, esta política hace hincapié en el cambio de las contraseñas de las otras máquinas. Ciertos técnicos no saben que los usuarios emplean con frecuencia la misma contraseña en diversos computadores. Los demás computadores correrán también un riesgo significativo a menos que se cambien todas las contraseñas.

Políticas Relacionadas: “[Sospecha de Intrusión en los Sistemas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Cambio de Contraseña de Usuario Privilegiado Comprometida

Política: Si un intruso u otro usuario no autorizado ha comprometido una cuenta privilegiada, todas las contraseñas de ese sistema deben ser cambiadas de inmediato.

Comentario: Esta política informa a los administradores de sistemas y otros en sistemas informáticos que todas las contraseñas se encuentran potencialmente comprometidas si el identificador de usuario privilegiado está comprometido. Esto se debe a que los usuarios privilegiados pueden establecer y modificar los privilegios de cualquier otro usuario del sistema afectado. Las contraseñas de todos los identificadores de usuario deben cambiarse de inmediato para evitar que un usuario no autorizado obtenga, de nuevo, acceso al sistema. Esta política es sólo un arreglo rápido y no puede mantener al intruso fuera del sistema afectado si ha modificado el software del sistema operativo. Se pueden utilizar otros mecanismos de control para detectar cambios en el sistema operativo.

Políticas Relacionadas: “[Cambios de Contraseña Luego de Estar Comprometido el Sistema](#)” y “[Cambios de Seguridad Despues de Estar Comprometido el Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Autentificación de Contraseña en Persona

Política: El usuario debe ser autenticado en persona a fin de obtener una contraseña nueva o modificada.

Comentario: Esta política garantiza que las contraseñas no serán entregadas a personas no autorizadas. Muchas personas han hecho uso de la ingeniería social para engañar a otras personas y hacer que les entreguen las contraseñas vía telefónica. Para evitar la divulgación inadecuada de contraseñas, ciertas empresas solicitan una prueba de identidad o pueden enviarlas en paquetes postales seguros. Esto significa que las contraseñas quedan automáticamente escritas en sobres pre-cerrados con papel carbón adherido, mediante impresoras de impacto sin cinta, lo cual evita que personas no autorizadas puedan ver las contraseñas. En caso de que un usuario deba obtener una contraseña durante una emergencia, ciertas empresas requieren que el solici-

tante demuestre su identidad, suministrando información que sólo él debería conocer. Algunas organizaciones piden varios detalles personales, tales como el nombre de soltera de la madre, el número de empleado o el número de placa del automóvil.

Políticas Relacionadas: “Envío de Contraseñas por Correo,” “Contraseñas Compartidas,” “Contraseñas Iniciales,” y “Códigos de Identificación para Soporte Técnico”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

11. Divulgación de Contraseñas

Política: Los administradores de seguridad deben divulgar las contraseñas a un usuario que suministre dos pruebas definitivas que comprueben su identidad, sólo si se le asigna un nuevo identificador de usuario, si el usuario involucrado ha olvidado o colocado erróneamente la contraseña, o si la desactivó sin querer.

Comentario: El propósito de esta política es aclarar cuándo y cómo los administradores de seguridad pueden divulgar una contraseña. Existen muchos casos en los que se emplea ingeniería social para hacer que los administradores de seguridad revelen la contraseña por vía telefónica. Esta política permite a un administrador de seguridad revelar la contraseña por vía telefónica, siempre que se suministre una prueba de identificación adecuada. Este proceso de suministro de contraseñas por vía telefónica resulta ventajoso, aunque menos seguro que pedir al usuario asistir en persona. En algunos casos, podría ser necesaria una contraseña fija o un número de identificación personal para activar la tarjeta que genera las contraseñas dinámicas. Para que sea realmente efectiva, la política requiere estar acompañada de varias políticas relacionadas, tales como requerir la modificación de contraseñas recientemente asignadas durante la primera sesión, en el momento en que sean utilizadas. Esta política supone que el término “administrador de seguridad” ha sido definido dentro de la organización.

Políticas Relacionadas: “Sospecha de Divulgación de Contraseña” y “Contraseñas Compartidas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Identificación Positiva para Uso del Sistema

Política: Todos los usuarios deben quedar identificados positivamente, antes de que puedan utilizar cualquier recurso de sistemas de computación multiusuario o de comunicaciones.

Comentario: La identificación positiva incluye comúnmente los identificadores de usuario y sus contraseñas fijas. Sin embargo, puede incluir también la biometría, sistemas para devolver llamadas, tarjetas de contraseñas dinámicas o certificados digitales. Igualmente, la definición precisa de identificación positiva puede variar de acuerdo con la plataforma o tecnología. Por ejemplo, tener acceso a los computadores que se esconden detrás del cortafuego de Internet podrá requerir de contraseñas dinámicas, además de las contraseñas fijas, mientras que el hacer uso de una tarjeta de crédito a través del teléfono requerirá solamente de una contraseña fija. La definición precisa de identificación positiva puede omitirse de esta política, de manera deliberada, de modo que la tecnología pueda cambiar con el tiempo, sin necesidad de efectuar cambios correspondientes en la política. Ciertas organizaciones querrán agregar palabras a la política, lo cual hace que el departamento de Seguridad Informática será el que decida cuándo se llega a la definición precisa del término “identificación positiva”. La duración prolongada de esta política deshace la elaboración de una política clara y sin ambigüedades. Esta política garantiza que ninguna persona no autorizada tendrá acceso a los computadores de la empresa o a los sistemas de comunicación. Esta política se vuelve cada vez más importante, a medida que las empresas adopten sistemas más interconectados. La red de área local de un departamento independiente plantea una vulnerabilidad limitante, pero cuando dicha red de área local se conecta con una red de área amplia, aumentan las necesidades que tienen los usuarios de identificarse positivamente. Asimismo, mientras se utilizan cada vez más pequeños sistemas para ejecutar aplicaciones de producción, esta política adquiere mayor importancia. Dentro del ambiente de sistemas pequeños, esta política puede requerir la optimización de ciertos sistemas operativos de red o sistemas operativos de estaciones de trabajo, a fin de dar soporte a sólidos controles de acceso.

Políticas Relacionadas: “Mecanismo Único de Acceso” e “Identificación de Visitantes”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9.02.04 Revisión de Derechos de Acceso del Usuario

1. Reautorización de los Privilegios de Acceso de Usuario

Política: Los privilegios del sistema que otorga el jefe inmediato del usuario deben ser nuevamente evaluados cada tres meses, para determinar si necesitan los privilegios de sistema habilitados actualmente para realizar las tareas propias del trabajo que realiza el usuario.

Comentario: A medida que se modifiquen las tareas propias del usuario, debe ocurrir lo mismo con los privilegios del sistema correspondientes. Sin embargo, en muchos casos, los usuarios cambian de puesto de trabajo y no se notifica de estos cambios al departamento de Seguridad Informática y a otros, tal como ocurre con los administradores de sistemas que se encargan de cambiar los privilegios. Esta política mantiene actualizados los privilegios y se restringen a los requisitos actuales del empleo. Se requiere realizar revisiones periódicas para restringir los privilegios. Para poder implementar esta política, muchas empresas emiten un informe de privilegios por usuario. Este mensaje de correo electrónico o memorandum llega a manos del jefe del usuario, quien tiene un determinado

período de tiempo para dar una respuesta. En caso de que no se reciba ninguna respuesta, se harían llamadas telefónicas, o se haría un seguimiento, para garantizar que el jefe realmente revisó el listado de privilegios. En los ambientes de alta seguridad, si el jefe no responde de manera oportuna, los privilegios del usuario podrían quedar revocados, hasta que el jefe los vuelva a autorizar. No hay nada de especial en el período de tres meses, ya que dentro de un ambiente de baja seguridad, este podría ser de seis meses, pero por lo general no debe ser superior a dicho período de tiempo. En algunos casos, las organizaciones querrán agregar las palabras "Todos los privilegios innecesarios quedarán revocados", al final de la política.

Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer," "Vencimiento de los Identificadores de Usuario," y "Reportes de Distintivos de Identificación"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9.03 Responsabilidades del Usuario

9.03.01 Utilización de Contraseñas

1. Estructura de las Contraseñas

Política: Los empleados no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

Comentario: El problema que se encuentra con mayor frecuencia en los sistemas de seguridad es el error humano, y la selección de contraseñas fijas que se pueden deducir con facilidad es uno de los más comunes relacionados con la seguridad. Esta política informa a los usuarios que deben seleccionar contraseñas que sean difíciles de deducir por personas no autorizadas. Lo ideal es que esta política se pueda ejecutar automáticamente, mediante cambios administrados por el sistema, y se debe invocar al software correspondiente cada vez que los usuarios seleccionen nuevas contraseñas. Se

pueden agregar a esta política otros aspectos específicos sobre qué constituye una contraseña de fácil deducción. Por ejemplo, se podrían prohibir términos técnicos o médicos. Esta política y sus medidas de control relacionadas son particularmente importantes, si los usuarios emplean la misma contraseña en múltiples sistemas. Esta política podría expandirse para suministrar sugerencias adicionales en la construcción de contraseñas que sean difíciles de deducir, pero fáciles de recordar. Por ejemplo, la política podría sugerir que los usuarios empleen métodos tales como:

- Hacer una sucesión de varias palabras que también se conoce con el nombre de frase de contraseña.
- Cambiar una palabra hacia arriba, hacia abajo, hacia la izquierda o hacia la derecha en una fila del teclado.
- Mover caracteres de una palabra un determinado número de letras del alfabeto, arriba o abajo.

- Transformar una palabra regular, de acuerdo con un método específico, como convertir una que otra letra en un número que refleje su posición en la palabra.
- Combinar puntuación o números con una palabra regular.
- Crear siglas provenientes de palabras de una canción, poema u otra secuencia conocida de palabras.
- Escribir mal una palabra de manera deliberada. Sin embargo, no utilizar los errores comunes de ortografía.
- Combinar una cantidad de hechos personales tales como fechas de nacimiento y colores favoritos.

Esta política esta destinada a su distribución entre usuarios finales. El uso de contraseñas difíciles de deducir disminuye las posibilidades de que otras personas las adivinen en el momento en que las estan tipeando y disminuye las posibilidades de que los usuarios las divulguen a otros.

Políticas Relacionadas: ‘Caracteres de las Contraseñas,’ ‘Contraseñas Cíclicas,’ ‘Configuración de Modem para Llamadas Discadas Entrantes,’ y ‘Sospecha de Divulgación de Contraseña’

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Contraseñas Cíclicas

Política: Los usuarios no deben crear contraseñas fijas que combinen un conjunto de caracteres no cambiantes con un conjunto de caracteres que cambien de manera predecible.

Comentario: A menudo, los usuarios se molestan porque los sistemas de contraseñas les exigen cambiar frecuentemente sus contraseñas. En su esfuerzo por lidiar con estos sistemas con mayor facilidad, a menudo los usuarios emplean contraseñas que cambian sólo de manera parcial. Una de las técnicas que utilizan se denomina contraseñas cíclicas, que permite a los usuarios seguir utilizando la misma contraseña básica, variando sólo una parte de la contraseña, para satisfacer un proceso automatizado que compara las contraseñas viejas con las nuevas, a fin de garantizar que no se vuelvan a utilizar las contraseñas anteriores. Este enfoque prevalece particularmente entre los usuarios que deben ingresar al sistema de diferentes computa-

dores. Esta política prohíbe a los usuarios utilizar este enfoque. Si bien los sistemas de registro único facilitan aún más a los usuarios el proceso de ingreso al sistema de un computador, la seguridad de la red y de los sistemas conectados se reducirán notablemente si los usuarios emplean contraseñas cíclicas.

Políticas Relacionadas: ‘Histórico de Contraseñas,’ ‘Reutilización de Contraseñas,’ y ‘Estructura de las Contraseñas’

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Almacenamiento de Contraseñas Legibles

Política: No se deben almacenar contraseñas fijas legibles dentro de archivos agrupados en lotes, comandos de inicio de sesión, macros de software y claves de funcionamiento de terminales en computadores que no tengan control de acceso, o en otras ubicaciones en las que las personas no autorizadas las pudieran descubrir o utilizar.

Comentario: Esta política evita que las contraseñas legibles caigan en manos de personas no autorizadas. Algunos usuarios almacenan sus contraseñas en varias ubicaciones que los computadores pueden leer. Aunque estos procedimientos ayudan a ahorrar tiempo, exponen el sistema involucrado a un acceso no autorizado. Las personas que irrumpen normalmente en los sistemas, verifican las claves de funcionamiento de los terminales, registros de ingresos al sistema y ubicaciones similares de las contraseñas. A menudo este enfoque resulta muy efectivo. Esta política se aplica igualmente a otros parámetros de seguridad además de las contraseñas, tales como las claves de cifrado, los parámetros de semillas de generadores numéricos seudoaleatorios, números de identificación personal y vectores de inicialización. Los parámetros de seguridad son una sucesión de caracteres que controlan un proceso de seguridad, tales como los que se utilizan cuando se ingresa al servidor de una red local. Debido a que éste abarca un área en la que los usuarios finales pueden ocasionar daños considerables no intencionales, esta política se aplica particularmente a los usuarios finales que emplean computadores personales, estaciones de trabajo y sistemas cliente-servidor. Esta política indica un procedimiento que es inconsistente con las características disponibles en algunos paquetes de software de comunicaciones. Estos sistemas permiten a los usuarios almacenar contraseñas en los registros de acceso al sistema. Para que esta política sea efectiva, los

usuarios deben adiestrarse respecto de cómo utilizar dichos paquetes de software sin guardar sus contraseñas en los registros de acceso al sistema.

Políticas Relacionadas: “Divulgación Pública de Contraseñas,” “Escritura de Contraseñas,” y “Contraseñas Legibles”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

4. Contraseñas en Distintos Sistemas

Política: Los usuarios de computadores deben emplear distintas contraseñas en cada uno de los sistemas para los que se les ha otorgado el acceso.

Comentario: Esta política evita que los usuarios utilicen una sola contraseña y expongan todos los identificadores de usuario ante personas no autorizadas que tratan de obtener el acceso. Si un hacker descubriese una contraseña fija a través de la deducción de la misma o la recuperase a través de un dispositivo de espionaje, todos los sistemas a los que la persona tenga acceso con la misma contraseña quedarían comprometidos. Esta política estimula a los usuarios a escribir sus contraseñas, debido a que muchos de ellos cuentan con muchas contraseñas distintas. Una política de este tipo puede ocasionar también una resistencia importante por parte de los usuarios, debido a que ellos tratan de simplificar su vida, empleando la misma contraseña en múltiples lugares. Esta política es adecuada únicamente para ambientes de alta seguridad. Una de las propuestas más beneficiosas es el uso de un frente, que también se conoce con el nombre de sistema de inicio único de sesión, el cual requiere que la persona ingrese al sistema una sola vez.

Políticas Relacionadas: “Mecanismo Único de Acceso,” “Divulgación Pública de Contraseñas,” y “Contraseñas en Distintos Sistemas — Permiso”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

5. Contraseñas en Distintos Sistemas — Permiso

Política: Los usuarios no deben utilizar la misma contraseña en múltiples sistemas de computadores, a menos que el departamento de Seguridad Informática les haya informado que el hacerlo no comprometerá de manera indebida la seguridad del sistema.

Comentario: Esta política requiere que el usuario obtenga un permiso, en lugar de crear una prohibición de utilizar la misma contraseña. Para algunos usuarios con menos privilegios en el sistema, no representaría una grave vulnerabilidad al sistema utilizar la misma contraseña en sistemas múltiples. Esta política debe reservarse para ambientes de alta seguridad.

Políticas Relacionadas: “Contraseñas en Distintos Sistemas” y “Mecanismo Único de Acceso”

Política Dirigida a:Todos

Ambientes de Seguridad:Altos

6. Sospecha de Divulgación de Contraseña

Política: Todo usuario debe cambiar su contraseña de inmediato si sospecha la divulgación de ésta o si sabe que ha sido divulgada a una persona no autorizada.

Comentario: El principio básico de los sistemas seguros que está detrás de esta política es que únicamente el usuario debe conocer su contraseña. Esta política supone que todos los usuarios tengan sus propios identificadores de usuario. Si se ha divulgado la contraseña a otra persona, o si sólo se sospecha de ello, se debe cambiar la contraseña de inmediato. Esta política implica que los usuarios pueden modificar sus contraseñas en cualquier momento. En caso de que esto no sea posible por razones técnicas o administrativas, un administrador de seguridad podría reiniciar la contraseña del usuario involucrado. Si se utiliza esta última opción, cerciórese de que la contraseña resultante la conozca solamente el usuario. El administrador del sistema puede emitir una nueva contraseña que el usuario debe modificar la próxima vez que ingrese al sistema.

Políticas Relacionadas: “Contraseñas Iniciales,” “Cambios de Seguridad Despues de Estar Comprobado el Sistema,” “Cambios Obligatorios de Contraseña,” y “Sincronización de los Intervalos de Cambios de Contraseñas”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

7. Divulgación Pública de Contraseñas

Política: No se deben escribir las contraseñas ni abandonarlas en sitios donde personas no autorizadas pudieran descubrirlas.

Comentario: El descubrimiento de contraseñas escritas y abandonadas en la primera gaveta de un escritorio, pegadas a la pantalla de una computadora o en cierto lugar llamativo es una forma sorprendentemente común que utilizan los atacantes para irrumpir en los sistemas de computación. Muchos usuarios no toman en cuenta estos riesgos, a menos que la administración los alerte al respecto. Esta política no indica que los usuarios no deben escribir sus contraseñas, sino que no deben dejarlas escritas y abandonadas en algún lugar donde otras personas pudieran encontrarlas. Esta política podría modificarse para convertirse en una política más estricta que prohíba en lo absoluto a los usuarios escribir sus contraseñas. Sin embargo, los usuarios lo hacen de todos modos en muchas partes. Esta política reconoce la realidad de los procedimientos comunes referentes a la escritura de contraseñas.

Políticas Relacionadas: “[Contraseñas Generadas por el Sistema](#),” “[Escritura de Contraseñas](#),” y “[Contraseñas en Distintos Sistemas](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Proximidad de Contraseñas a Dispositivos de Acceso

Política: Los usuarios no deben nunca escribir o de otro modo registrar una contraseña legible y almacenarla cerca de los dispositivos de acceso a los que pertenece.

Comentario: Esta política informa a los usuarios que no deben guardar una contraseña cerca de un dispositivo de acceso al cual pertenece. Esto ocurre a menudo con los computadores portátiles y con los usuarios que registran las contraseñas y los números de acceso telefónico que se encuentran dentro de sus computadores portátiles. Para obtener el acceso no autorizado a computadores remotos, el ladrón sólo necesita examinar estos archivos. Asimismo, no deberían registrar en los propios dispositivos los números de identificación personal que son necesarios para inicializar las tarjetas portátiles o tarjetas inteligentes que contienen contraseñas dinámicas. Esta política sustenta la "autenticación de dos factores" o el uso de dos técnicas que autentifiquen la identificación de un usuario. Si se combina la contraseña con el dispositivo, lo que era una autenticación de dos factores se convierte en autenticación de un solo factor.

Políticas Relacionadas: “[Credenciales Portátiles de Identificación](#)” y “[Escritura de Contraseñas](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9. Contraseñas en Software de Comunicaciones

Política: Los usuarios no deben guardar en ningún momento contraseñas fijas en programas de comunicaciones con sistema de disco duro, exploradores de Internet o software relacionado con comunicaciones de datos.

Comentario: Esta política evita que los usuarios empleen las características amigables de muchos programas de comunicaciones. Una de las funciones permite guardar las contraseñas fijas para referencia futura. Aunque estas contraseñas se encuentran normalmente guardadas en forma de cifrado y están ocultas al momento de escribirlas en la pantalla, de modo que las personas no autorizadas no las puedan leer, las personas no autorizadas que tienen acceso al computador donde se encuentra instalado el software, pueden hacer uso de ellas. De este modo, pese a que no se revelan las contraseñas, pueden utilizarse para obtener acceso no autorizado al sistema. Esta política es de especial importancia para aquellos computadores portátiles que no tienen el beneficio de controles de acceso físico para su protección. Lo ideal es que el software de comunicaciones sea modificado para evitar que los usuarios empleen esta característica. No obstante, este tipo de modificación no es práctica en la mayoría de las organizaciones. La única alternativa es prohibir a los usuarios emplear una característica que, de otro modo, se consideraría conveniente y deseable. Si los usuarios guardan sus contraseñas fijas en un computador, desde la perspectiva de un diseño seguro de sistemas, la posesión de la misma podría ser todo lo que se necesita para obtener acceso a un computador remoto, pero si los usuarios guardan estas contraseñas fijas en su cerebro, el acceso al sistema podría lograrse solamente con dicha posesión acompañada del suministro de una contraseña secreta.

Políticas Relacionadas: “[Almacenamiento de Contraseñas Legibles](#)” y “[Recuperación de Contraseñas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Cookies para Inicios Automáticos de Sesión

Política: Los usuarios de computadores de la Empresa X deben negar todas las ofertas hechas por el software para colocar cookies en su computador, de modo que puedan ingresar al sistema de manera automática, la próxima vez que visiten un sitio específico en Internet.

Comentario: Esta política evita que los usuarios acepten los cookies de ingreso al sistema que pudieran utilizar personas no autorizadas para obtener acceso al sistema, ordenar productos u obtener información restringida. Un cookie es un pequeño archivo que contiene información de un usuario específico y se encuentra ubicado en el disco duro del usuario. Este puede utilizarse para identificar a ese usuario de una manera particular. El uso de cookies de ingreso al sistema simplifica y sustituye el proceso tradicional de ingreso. Muchos comerciantes de Internet creen que les está prestando a los usuarios un gran servicio, al momento en que ofrecen colocar este tipo de cookie en los computadores de los usuarios. El uso de los cookies de ingreso disminuye la seguridad del sistema, debido a que sustituye la información que conoce el usuario con una inmediación material simple a un computador remoto. Muchos usuarios sólo piensan en el momento en que ésta se guardaría o en cómo reduce la necesidad de recordar una contraseña. No toman en cuenta cómo otras personas se hacen pasar por ellos y tal vez, cometan delitos informáticos. Adicionalmente, estos usuarios, por lo general, no piensan en otras cosas que pudieran hacer estos cookies de ingreso, por ejemplo, crear un registro detallado de sus actividades en Internet. Si los computadores de los usuarios tienen controles de acceso muy sólidos, tales como discos duros con cifrado y contraseñas para arrancar el computador, entonces no será necesaria la restricción que se describe en esta política.

Políticas Relacionadas: “[Información Personal Incluida](#)” y “[Contraseñas en Software de Comunicaciones](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

11. Tarjetas de Contraseñas Dinámicas

Política: Las tarjetas portátiles con contraseñas dinámicas no deben guardarse en el mismo maletín de los computadores portátiles que se utilizan para obtener acceso remoto a las redes de la Empresa X.

Comentario: Esta política evita que la comodidad pase por encima de la seguridad. Sin estas instrucciones, los usuarios guardarían las tarjetas de contraseñas dinámicas en el mismo maletín del computador. En algunos casos, estas tarjetas no poseen contraseñas fijas habilitantes, lo cual significa que la posesión de la tarjeta y del computador sería suficiente para obtener acceso no autorizado al sistema. Aunque se requiriera una contraseña fija para habilitar la tarjeta, se reducirían notablemente los recursos necesarios para comprometer la seguridad del sistema si las tarjetas están junto al computador al que pertenecen. Esta política alienta la causa de la autenticación multi-factor de usuario, la cual exige la presencia de distintas cosas para otorgar acceso al sistema e incluyen algo que el usuario sabe, algo que el usuario tiene, algo que el usuario puede hacer o algo que el usuario es. A los usuarios generalmente no les gusta, pero cuando la entienden están más dispuestos a cumplir políticas como ésta. Esta política cobra mayor importancia, ahora que el robo de computadores portátiles es más común. El sistema de contraseña dinámica mencionado en la política podría usarse tanto en el computador portátil como en la máquina remota, o sólo en esta última.

Políticas Relacionadas: “[Distintivos de Acceso Extraviados](#)” e “[Identificación Positiva para Uso del Sistema](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

12. Números de Identificación Personal

Política: Todos los números de identificación se deben construir con las mismas reglas aplicables a las contraseñas fijas.

Comentario: Esta política informa tanto a los usuarios finales como a los administradores del sistema que no deben bajar la guardia al seleccionar o crear números de identificación personal, que también se conocen con el nombre de PIN, por sus siglas en inglés. Muchas personas consideran que sus PIN no necesariamente tienen que ser difíciles de deducir, debido a que los PIN a menudo forman parte de un esquema multi-factor de autenticación del usuario, que requiere del PIN y de un segundo elemento para otorgar acceso al sistema. La concepción errada en torno al papel que cumple un PIN y la selección resultante de un PIN de fácil deducción facilita aún más al atacante el acceso no autorizado al sistema. Es obligatorio y necesario tener un PIN de difícil deducción, debido a que estos constan a menudo de tan sólo cuatro caracteres, lo cual significa que no

hay muchas combinaciones posibles. Esto hace que los PIN estén sujetos a ataques brutales de fuerza en donde se intentan todas las combinaciones y se vuelve particularmente importante un mecanismo de cierre, después de cierto número de intentos incorrectos para ingresar al sistema. Debido a que los PIN sólo incluyen números, ciertas reglas para la creación de contraseñas son poco importantes. Sin embargo, ese mismo propósito se aplica los PIN, para hacer que éstos sean difíciles de deducir.

Políticas Relacionadas: “Autentificación de Usuario Que Accede Vía Teléfonica” e “Intentos de Contraseñas por Discado”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

13. Escritura de Contraseñas

Política: Los usuarios no deben escribir sus contraseñas, a menos que hayan ocultado las mismas de manera efectiva en caracteres no relacionados similares o que hayan utilizado un sistema de códigos para ocultar la contraseña.

Comentario: Esta política proporciona lineamientos específicos con respecto a las formas adecuadas de escribir las contraseñas, si es que las escriben. Con el reciente crecimiento desmedido en la cantidad de contraseñas que los usuarios deben recordar, junto con la necesidad de hacer cambios en algunas de estas contraseñas en forma periódica, los usuarios se sienten a menudo como si no tuvieran otra opción que escribir sus contraseñas. Al mismo tiempo, la escritura de contraseñas puede ser una forma sencilla de permitir que personas no autorizadas obtengan acceso al sistema. Esta política propone un balance práctico para resolver estos objetivos en conflicto. Los procedimientos de codificación que pudieran mencionarse incluyen un método en donde se pueden colocar las contraseñas en una cinta, en un lugar llamativo, puesto que ya han sido alteradas a través de algún enfoque normalizado.

Políticas Relacionadas: “Divulgación Pública de Contraseñas” y “Contraseñas Legibles”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

14. Contraseñas Compartidas

Política: Nunca se deben distribuir ni revelar las contraseñas a ninguna persona distinta al usuario autorizado.

Comentario: En el momento en que los usuarios divulguen sus contraseñas a cualquier otra persona, comprometen los controles de acceso del sistema en forma negligente, y hacen que los registros de la actividad del usuario tengan menor utilidad. Es importante que los usuarios se guarden sus contraseñas exclusivamente para sí. Esta política les recuerda que deben proceder de esa manera. La política podría llegar a mencionar que el hecho de mantener en secreto su contraseña significa que es la manera en que un usuario puede evitar responsabilidades por las acciones de otra persona. En muchas organizaciones con ambientes de sistemas pequeños, prevalece tradicionalmente una actitud casual hacia la seguridad. Una política de este tipo podría contrarrestar dicha actitud.

Políticas Relacionadas: “Autentificación de Contraseña en Persona,” “Límite al Acceso Diario,” y “Contraseñas de Control de Acceso al Sistema”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

15. Uso de Contraseñas por Terceros

Política: Los usuarios no deben suministrar sus identificadores de usuario ni sus contraseñas a ningún tercero, incluyendo entre otros, agregadores de datos y servicios de resumen/formato de datos.

Comentario: Esta política desestimula a los usuarios a utilizar una nueva especie de servicios prestados por terceros denominados proveedores de servicio de agregado de datos. Estas personas dedicadas a agregar datos en forma automática reúnen la información de varias organizaciones a través de Internet y luego las presentan al usuario en forma resumida. Por ejemplo, ciertas personas dedicadas a agregar datos combinarán la información de la cuenta de un corredor de valores, una cuenta bancaria y una cuenta de su plan de pensiones, todo esto manejado por distintas organizaciones, y luego presenta un balance actual consolidado al usuario. Aunque estos servicios son cómodos y funcionan real y adecuadamente, el cliente involucrado debe divulgar su identificador de usuario y su contraseña a la persona encargada de agregar los datos, de modo que pueda actualizar y combinar las información de diferentes fuentes. La emisión de cualquier información que autentifique la identidad del

usuario a un tercero constituye un procedimiento peligroso, con lo cual se abre una variedad de riesgos que, de lo contrario, no sería necesario tomar en consideración. Otros métodos, como el formateo inusual de la información de la cuenta en pantalla, se pueden utilizar para dificultar aún más o imposibilitar las rutinas de recopilación de datos de las personas encargadas de agregarlos. Desgraciadamente, estas tácticas pueden dificultar aún más a los usuarios autorizados sus intentos por recopilar su propia información automáticamente y cargarla en programas de contabilidad. El uso de tecnologías de autenticación de usuarios más sofisticadas, tales como las contraseñas dinámicas, es quizás la mejor manera de garantizar la no utilización de "agregadores" de datos.

Políticas Relacionadas: “Prohibición de Invasión de Privacidad a Través de Terceros” y “Números de Cuenta Bancaria”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

16. Identificadores Personales de Usuario — Responsabilidad

Política: Los usuarios deben responsabilizarse de toda la actividad realizada con sus identificadores personales de usuario y no deben permitir que otras personas realicen cualquier actividad con éstos o que realicen actividad alguna con identificadores que pertenezcan a otros usuarios.

Comentario: Esta política aclara que está prohibido compartir los identificadores de usuario y las contraseñas relacionadas. Si los usuarios comparten sus identificadores de usuario y contraseñas, los registros no reflejarán su verdadera identidad y resultarán menos útiles para acciones disciplinarias, procesamientos judiciales e investigaciones. Los controles de privilegios específicos de un usuario tienen poco significado cuando los usuarios comparten sus identificadores de usuario y sus contraseñas. Asimismo, esta política prohíbe la "violación" de sistemas externos con la ayuda de los sistemas de la Empresa X. En ciertos ambientes de computación, los identificadores individualizados de usuario reciben el nombre de cuentas o, en ocasiones, UID. Esta política no está diseñada para organizaciones, tales como escuelas, que emplean identificadores de usuario grupales.

Políticas Relacionadas: “Cuentas Unicas de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Compartir Códigos de Acceso

Política: Las cuentas de computación, los identificadores de usuario, las contraseñas de red, los números de identificación personal en la casilla de correos de voz, los números de tarjetas de crédito y otros códigos de la Empresa X, no debe utilizarlos ninguna otra persona distinta a aquélla para quien fueron emitidas originalmente.

Comentario: Esta política establece que bajo ninguna circunstancia se deben distribuir los códigos de acceso al sistema informático. Esta política es distinta de las políticas relacionadas, ya que se refiere a todos los códigos de acceso y no sólo a los identificadores de usuario y las contraseñas. Por lo tanto, se aplica a las nuevas tecnologías que una organización despliega a futuro y no requiere de modificación alguna en el momento en que éstas sean introducidas al sistema. Esta política hace que los ingresos al sistema y otros registros computarizados, tales como los recibos telefónicos, sean más confiables, debido a que es muy probable que las entradas serán con toda probabilidad atribuibles a las personas autorizadas. La política refuerza el concepto de responsabilidad personal.

Políticas Relacionadas: “Identificadores Personales de Usuario — Responsabilidad” y “Cuentas Unicas de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Prueba de los Controles del Sistema Informático

Política: Los empleados no deben probar o tratar de comprometer los controles internos, a menos que la gerencia de Seguridad Informática lo apruebe específicamente con antelación y por escrito.

Comentario: Esta política echa por tierra las excusas que a menudo se invocan para cometer delitos informáticos, ya que los atacantes podrían decir que ellos estaban simplemente probando el sistema de control, para ver si estaban en capacidad de mejorarlo. Los auditores internos ya tienen esta aprobación en la declaración de la misión departamental y deben continuar con las pruebas de estos controles. Esta actividad requiere de un control y desempeño estricto de manera confidencial, siempre que existan méritos para probar los controles regularmente, a fin de definir sus

debilidades. En líneas generales, esta política se aplica a la ejecución de paquetes de software comercial y de dominio público para interrumpir los controles del sistema. Esta política evitará que los usuarios manejen programas que violen los sistemas, a menos que tengan la aprobación de la gerencia. Asimismo, esta política prohíbe los ataques de penetración al sistema, a menos que la administración los apruebe con antelación.

Políticas Relacionadas: “Comprometer Mecanismos de Seguridad para los Clientes,” “Intentos No Autorizados de Acceso Físico,” “Actividades del Hacker,” y “Evidencia de Delito o Abuso Informático”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

19. Explotación de las Vulnerabilidades de la Seguridad del Sistema

Política: Los usuarios no deben explotar los puntos vulnerables o las deficiencias en la seguridad de los sistemas informáticos, para dañar estos sistemas o la información, obtener recursos más allá de aquellos autorizados, quitar los recursos a otros usuarios u obtener acceso a otros sistemas para los que no han recibido la autorización adecuada.

Comentario: Esta política aclara que los usuarios no deben aprovecharse de los puntos vulnerables de la seguridad informática y de sus deficiencias, incluso si tuviesen conciencia de dichos problemas. Un ejemplo de dicho problema incluye el tener conocimiento de una contraseña especial que permita a un usuario realizar operaciones que, de otro modo, no podría. En el sentido más amplio de la palabra, lo que indica esta política es que se otorgan a los usuarios únicamente los privilegios que explícitamente reciben. Si pueden hacer alguna otra cosa más por problemas de seguridad, no están autorizados para aprovecharse de estos problemas. Tal como está indicado, la política incluye los errores que cometen los administradores de sistemas, por ejemplo, si proporcionan privilegios adicionales a un usuario. Esto constituye decididamente una deficiencia relacionada con el despliegue de los controles, aunque este ejemplo puede no incluir la vulnerabilidad de un control.

Políticas Relacionadas: “Informes de Incidentes” y “Hardware y Software de Diagnóstico”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

20. Construcción de Contraseñas de Correo Voz

Política: Las contraseñas para correo de voz no deben ser obligadas a cumplir las normas de construcción de contraseñas establecidas por la Empresa X, pero los usuarios deben seleccionar una contraseña que sea distinta a su extensión telefónica, su número de oficina, su número de empleado y cualquier otro número que pudiera deducirse con facilidad.

Comentario: Esta política aclara la razón por la que el número mínimo de caracteres en las contraseñas de correo de voz es normalmente menor a la del número mínimo que tienen las contraseñas de computadores. Ciertos usuarios se han quejado de que sus organizaciones no siguen sus propias normas, al no requerir que el sistema de correo de voz cumpla con una norma de construcción de contraseñas. Esta política explica que no es necesario que se cumpla dicha norma, pero al mismo tiempo refuerza la necesidad de seleccionar una contraseña sólida y difícil de deducir. La indicación de un número mínimo de dígitos en una contraseña de correo de voz pudiera aumentar con esta política. Este tipo de contraseña es un número de identificación personal, debido a que sólo se dispone de un número limitado de dígitos. Se recomienda que las contraseñas del correo de voz tengan al menos ocho dígitos, debido a que el número de posibilidades de que una contraseña de correo de voz tenga una cierta cantidad de dígitos es bastante limitado.

Políticas Relacionadas: “Excepciones a las Políticas,” “Estructura de las Contraseñas,” e “Información Sensible en Máquinas Contestadoras”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

21. Cuentas Únicas de Correo Electrónico

Política: Los empleados no deben utilizar una cuenta de correo electrónico que haya sido asignada a otra persona, ya sea para enviar o recibir mensajes.

Comentario: Esta política tiene como propósito reforzar la premisa de que cada usuario debe tener su propio identificador de usuario de correo electrónico y que, bajo ninguna circunstancia, los usuarios no deben compartir estos identificadores. Esta política prohíbe implícitamente las cuentas grupales, una forma preferida por ciertas organizaciones para ahorrarse los costos de administración del sistema. La idea fundamental de esta política se aplica a otros tipos de identificadores de usuario, aun cuando esto es específico

del correo electrónico. La política mantiene la precisión y eficacia de los registros de los sistemas de correo electrónico, mientras disminuye la confusión que pudiera surgir cuando alguna persona utiliza la cuenta de otra persona. Adicionalmente, la política apoya el cumplimiento de restricciones en los privilegios que pudieran estar relacionados con cuentas específicas. Una política escrita de este tipo establece también que usar el correo electrónico de otros está prohibido, lo que conlleva a la justificación de despidos y de otras maneras menos severas de castigo. Asimismo, esta política prohíbe una táctica preferida de aquellas personas que envían correos electrónicos comerciales en

bloque, sin hacer sido solicitados, a fin de evitar el rastreo de los mensajes hacia el verdadero autor que los originó.

Políticas Relacionadas: “Identificador Único de Usuario y Contraseña Obligatorios,” “Información Secreta en Correo Electrónico,” “Monitoreo de Mensajes de Correo Electrónico,” “Revisión de Mensajes de Correo Electrónico de Terceros,” y “Contraseñas de Control de Acceso al Sistema”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

9.03.02 Equipos de Usuario Desatendidos

1. Sesiones Activas Desatendidas

Política: Si el sistema de computación al cual están conectados o el cual están utilizando contiene información sensible, los usuarios no deben dejar desatendidos sus computadores personales, estaciones de trabajo o terminales sin salir del sistema o invocar un protector de pantalla.

Comentario: Esta política evita la divulgación no autorizada de información y su uso no autorizado. Esta política pone la responsabilidad en manos del usuario, en lugar de ordenarle la indicación de un período de inactividad, más allá del cual se puedan dar por terminado los trabajos. Por lo general, esta propuesta es menos efectiva que la conclusión automática de una sesión inactiva. Sin embargo, hace énfasis en el hecho de que los usuarios son los responsables de la seguridad de la información que tienen en sus manos. Las organizaciones no deben usar estas dos propuestas a la vez. En esta política, no existe un período aceptable durante el cual se dejen desatendidos los sistemas que contienen información sensible. En esta política, se pudiera proporcionar una palabra o dos que indique un período de tiempo determinado, como 15 minutos. No obstante, esto no es recomendable, porque requiere la sincronización de todas las máquinas del sistema. La referencia a la "salida del sistema" pudiera extenderse para incluir paquetes de control de acceso basados en contraseñas.

Políticas Relacionadas: “Cierre de Sesión Automático” y “Sistemas de Redes Desatendidos”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Sistemas de Redes Desatendidos

Política: En caso de que los computadores personales se encuentren conectados a una red, siempre deben estar fuera de sistema si se encuentran desatendidos.

Comentario: Esta política garantiza que los usuarios saldrán del sistema cuando dejen desatendidos sus computadores personales (PC), con la condición de que el PC se encuentra conectado a una red. La palabra "red" se utilizó en lugar de red de área local, red de área amplia, red telefónica con sistema de discado, u otros términos más restringidos. Esta política resulta particularmente importante en aquellos casos donde los PC cuentan con modem pero no con sistemas de control de acceso, en cuyo caso ninguna persona que marque un número telefónico con estos sistemas podrá tener acceso a los PC. La tarea que se menciona en esta política no dependería exclusivamente del usuario. El sistema se desconectaría en forma automática, luego de un determinado período de inactividad. Los usuarios deben salir del sistema al dejar sus PC, incluso contando con instalaciones para salir automáticamente de ella. Esta política supone que se está utilizando software de control de acceso en los computadores personales.

Políticas Relacionadas: “Sesiones Activas Desatendidas,” “Modem de Estaciones de Trabajo,” “Control de Acceso a Computadores de Red,” y “Cierre de Sesión Automática”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

9.04 Control de Acceso a la Red

9.04.01 Política para el Uso de los Servicios de Red

1. Descontinuación del Servicio

Política: La Empresa X debe reservarse el derecho a bloquear, ocultar, negar o descontinuar su servicio en cualquier momento y sin previo aviso.

Comentario: Esta política evita que terceras personas responsabilicen a la Empresa X por no seguir prestando servicios informáticos o servicios informáticos con ciertas características. Esta política informa a los usuarios que la empresa que presta su servicio en la red puede descontinuarlos o cambiarlos, en cualquier momento, sin previo aviso, para acelerar o mantener su propio negocio e intereses de seguridad. Esta política exonera de responsabilidad a la Empresa X por usos aguas abajo dependientes de su servicio que no hayan sido expresamente acordados por escrito. En líneas generales, una organización que ofrezca un servicio al público, como el de referencia de tiempo, podría utilizar esta política. Esta política permite que la empresa emisora descontinúe su servicio sin previo aviso, en caso de que un hacker haya comprometido los sistemas de soporte. Dicha descontinuación de servicio sería necesaria para el re establecimiento de un ambiente de computación confiable.

Políticas Relacionadas: “[Confirmación de Información de Pago](#)” y “[Esconder Transmisión de la Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Altos

2. Control de Acceso a Computadores de Red

Política: Si los empleados dejan encendidos sus computadores durante horas no laborables, y si están conectados a una red, los computadores deben estar protegidos por un sistema de control de acceso que cuente con la aprobación de la gerencia de Seguridad Informática.

Comentario: Esta política garantiza que las personas no autorizadas no obtendrán acceso a los sistemas de la Empresa X durante horas no laborables. Muchos hackers y demás atacantes del sistema se encuentran muy activos a esa hora. El ámbito de esta política podría resumirse en que debe haber un paquete de control de acceso en cada computador que esté conectado, si los computadores se encuentran conectados a una red externa. Asimismo, esta política podría aplicarse a todas

las redes, tales como una intranet, una extranet y una red telefónica de discado. La organización deseará suministrar ejemplos de distintos tipos de redes dentro de la estructura. Esta política podrá también desestimular la conexión a las redes, a menos que se hagan con antelación arreglos para la colocación de controles adecuados. Esta política constituye una respuesta directa a los problemas que ocurren con frecuencia en donde los usuarios finales mantienen encendidos sus computadores de un día para otro y, al mismo tiempo, tienen también encendido un modem conectado a la red. Si bien esto permite a los usuarios finales conectarse con los computadores de su oficina desde su casa o desde otro lugar, también permite a personas no autorizadas acceder al mismo computador. La vulnerabilidad de este procedimiento resulta particularmente grave cuando el computador se encuentra conectado a una red interna, como redes de área local, redes de área amplia o un sistema cliente-servidor.

Políticas Relacionadas: “[Modem de Estaciones de Trabajo](#)” y “[Respaldos Automáticos](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Autorización para Conexiones a Internet

Política: Los empleados no deben establecer ninguna conexión externa que pudiera permitir a los usuarios ajenos a la Empresa X obtener acceso a los sistemas informáticos de la misma, a menos que se obtenga una aprobación previa de la gerencia de Sistemas Informáticos.

Comentario: Esta política está dirigida a cubrir las conexiones a Internet y otras redes externas. El propósito de esta política es regular el establecimiento de conexiones a Internet. Sin una política como ésta, los usuarios podrían establecer su propia página web o establecer su propio sitio de protocolo para transferir archivos en Internet y en cualquier caso, es posible que la organización quede mal parada. Existe una necesidad de que dichas conexiones cumplan las medidas de seguridad normales y las convenciones de contenido y formato que establece la gerencia de Mercadeo o de Relaciones Públicas. Esta política alerta a los usuarios que pueden crear problemas de seguridad cuando se conectan con computadores externos.

Políticas Relacionadas: “Interconexión de Sistemas,” “Responsabilidades de Terceros en la Seguridad Informática,” “Conexiones a Internet,” y “Conexiones en Red con Organizaciones Externas”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Normas de Telefónicas Comunes

Política: Los servicios de conexión en la red suministrados por la Empresa X deben prestarse con base en un contrato como operadora y no como operadora común.

Comentario: Esta política evita la necesidad de suministrar acceso a la red y otros requisitos de operadora telefónica común, algunos de los cuales incluyen seguridad. Aun cuando la Empresa X podría tener una seguridad superior a la que se encuentra en los sistemas de telefonía común, esta política da una mayor flexibilidad a la administración de la Empresa X para decidir cómo quiere configurar y mantener su red. Es muy importante que el departamento Legal de la organización apruebe esta política, debido a que es de naturaleza legalista. Esta política es más general que la mayoría y se utiliza mejor como comentario introductorio antes de políticas más específicas. Otro de los propósitos de la política es establecer expectativas realistas del usuario, en cuanto al tipo de servicio y seguridad que serán prestados.

Políticas Relacionadas: “Servicios de Protección de Mensajes en Red” y “Sin Responsabilidad en Mensajes”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Acceso a la Red Interna

Política: Sólo los computadores suministrados por la Empresa X deben tener capacidad para acceder a la red interna de la Empresa X.

Comentario: Esta política separa a todos los computadores personales con acceso a la red interna de la Empresa X, lo cual significa que todos estos computadores cuentan con mecanismos de control de cambios basados en el sistema operativo que permiten a un administrador de sistemas remotos actualizar el software o su configuración. Sin embargo, los empleados que utilizan estos computadores no podrán actualizar ni el software ni sus configuraciones. Normalmente, la administración remota de computadores puede realizarse de manera automática, a través de un

programa automatizado para la distribución de software. Además de preservar el tiempo con el que cuenta el personal técnico, dicha propuesta evita infecciones mediante virus y gusanos, incompatibilidades debido a programas no autorizados y violaciones a las condiciones de la licencia del software otorgada por el proveedor del computador. Igualmente, esta propuesta permite que el software de autenticación extendida del usuario se agregue a cada computador personal autorizado y quizás el software de una red privada virtual. Este programa de autenticación podría incluir rutinas de exigencia/respuesta, rutinas con contraseñas dinámicas, biometría o un proceso de cifrado en una contraseña fija basada en tarjetas. Estas rutinas de software especializado en seguridad pueden utilizarse para bloquear a todos los computadores no autorizados, incluso si el usuario involucrado suministra correctamente el identificador de usuario y su contraseña fija.

Políticas Relacionadas: “Discos Flexibles” y “Equipo de Teletrabajo”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Derechos de Acceso a Internet

Política: Todos los tipos de acceso a Internet, con la excepción del correo electrónico, deben contar con autorización anticipada por escrito del gerente del departamento correspondiente que asegure que el usuario tiene una necesidad demostrable de dicho acceso.

Comentario: Muchas organizaciones proporcionan acceso total a Internet a todos los empleados de oficina, sin tomar en cuenta las ramificaciones de seguridad del acceso. Durante el proceso, estas personas crean problemas que incluyen menor productividad y divulgación de información confidencial y propia. Esta política se opone a las actitudes frecuentes de muchos empleados que afirman que el acceso a Internet es un beneficio del trabajo. Es probable que esta política no sea aceptable para una organización de alta tecnología, en donde se considera que el acceso a la tecnología más reciente es un beneficio adicional. Desde el punto de vista operacional, se podría implementar esta política, proporcionando a los empleados de oficina una serie de aplicaciones normales que incluyen un paquete de procesamiento de palabras, hoja de cálculo y programa para correos electrónicos. El acceso general a Internet puede suministrarse dentro de una biblioteca corporativa o en otras áreas comunes, lo cual hace más difícil que los usuarios malgasten el tiempo navegando en Internet.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

7. Restricción de Acceso a Internet

Política: El acceso a Internet debe otorgarse solamente a los empleados de la Empresa X que realicen investigaciones como parte regular de su trabajo.

Comentario: Esta política limita el acceso a las características web de Internet, y evita así una serie de problemas de seguridad. Dicha limitación reducirá, por ejemplo, el riesgo de infección por virus debido a contenido dinámico. Igualmente, esta limitación evitará que los empleados malgasten el tiempo navegando en la red mientras trabajan. Esta política reduce la necesidad de un software para seleccionar los contenidos a través de un cortafuego, pese a que lo más deseable es filtrar los mensajes y anexos de un correo electrónico.

Políticas Relacionadas: “Derechos de Acceso a Internet” y “Fuentes de Noticias en Internet”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

8. Sitios Web No Relacionados con Negocio

Política: Los sistemas informáticos de la Empresa X deben evitar rutinariamente que los usuarios se conecten a determinadas páginas web no comerciales.

Comentario: Esta política evita problemas, tales como los que resultan de acceder a las páginas web inadecuadas. Estas actividades podrían interpretarse como la creación de un ambiente hostil de trabajo, lo cual podría exponer a la empresa a demandas judiciales. La política también reconoce la existencia de nuevos productos que filtran la actividad en la web, manteniéndola dentro de ciertos límites. Dado que se agregan sitios con mucha rapidez a Internet, no es posible actualmente que estos programas eviten que los usuarios visiten todos los sitios prohibidos por la política. Como respuesta a esta realidad, los usuarios deberían salir del sitio y no continuar en el sitio prohibido.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones,” “Restricciones en Contenido de Mensajes,” y “Fuentes de Noticias en Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Bloqueo de Acceso a Sitios Ajenos al Negocio

Política: La Empresa X debe utilizar, como rutina, software que evite que los usuarios visiten cualquier página web en Internet que la administración considere censurable o claramente personal por su naturaleza.

Comentario: Esta política comunica a todos los usuarios que están conectados a Internet que no debe tener esperanzas de llegar a ninguna página web que pueda considerarse censurable o personal. Aun cuando esta política no menciona específicamente si la administración vigila las páginas web que los usuarios visitan, a menudo es buena idea declararlo de manera explícita a través de este tipo de políticas. La administración deseará actualizar el listado de páginas web prohibidas, de acuerdo con un registro que indique hacia dónde se dirigen los usuarios en Internet. Si en este registro se encuentran con frecuencia ciertas páginas web personales o censurables, éstas deben agregarse a la lista de páginas web bloqueadas. Este tipo de políticas puede utilizarse como un escudo para proteger a los administradores de sistemas de las quejas que tienen los usuarios, específicamente quejas sobre la imposibilidad de llegar a ciertas páginas web, tales como las de información noticiosa.

Políticas Relacionadas: “Control de Tráfico en Internet” y “Acceso de Usuarios a Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Descargas Grandes desde Internet

Política: Los usuarios de Internet no deben emplear facilidades de flujo de videos, de flujo de audio o descargar grandes archivos gráficos, a menos que el jefe inmediato del usuario lo apruebe con antelación.

Comentario: El propósito principal de esta política es fomentar la productividad entre aquellos empleados que tengan conexiones en Internet. Tener una conexión de alta velocidad en Internet puede resultar muy tentador para muchos empleados. Esta política evita que los empleados vean películas en línea, efectúen juegos en línea, escuchen radio mientras trabajan o descarguen grandes gráficos que no tienen relación con su trabajo. La declaración de esta política podría examinar un

documento que en ocasiones recibe el nombre de política de uso aceptable. Esta política no requiere de ninguna tecnología, como el software de monitoreo, aunque este software es a menudo recomendable.

Políticas Relacionadas:“Uso Personal del Teléfono” y “Registros de Uso de Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Identidad en Internet

Política: Los empleados no deben ocultar o falsificar su identidad al utilizar los sistemas informáticos o al llevar a cabo actividades comerciales de la Empresa X.

Comentario: El propósito de esta política es evitar que los empleados utilicen los sistemas de la Empresa X para realizar actividades cuestionables en Internet. Los registros del sistema resultarán considerablemente menos útiles sin la información de identidad válida de un usuario. Además, la falta de un medio de identificación podría estimular a que la gente realice cosas que de otra manera no haría. Uno de los principios fundamentales del diseño de sistemas seguros es que se debe obtener la identificación positiva del usuario antes de poder aplicar controles de acceso. Si no se ha establecido la identidad de un usuario, se disminuye la efectividad de los controles de acceso. Si los empleados desean ocultar su identidad, tal vez para un grupo de discusión de especial interés, siempre lo pueden hacer con el identificador personal de usuario que pueden obtener de un proveedor de servicios de Internet. Esta política prohíbe el uso de reenviadores de correos electrónicos, los cuales supuestamente han sido utilizados para cometer delitos y actividades cuestionables.

9.04.02 Vía Exigida

1. Control de Acceso a los Computadores Conectados a la Red

Política: Todos los computadores de la Empresa X que lleguen a las redes de terceros deben estar protegidos mediante un sistema de control de acceso de privilegios autorizado por la gerencia de Seguridad Informática.

Comentario: El objeto de esta política es aclarar cuáles sistemas deben tener un sistema de control de acceso basado en contraseñas. Este tipo de sistema de control de acceso está excluido deliberadamente de esta

Políticas Relacionadas:“Acceso Entrante a Internet”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

12. Propiedad Intelectual

Política: Al acceder a Internet utilizando los sistemas de la Empresa X, los empleados deben republicar o reproducir material sólo después de obtener el permiso de la fuente, citar material de otras fuentes sólo si proceden a identificar las mismas o revelar información interna de la Empresa X en Internet sólo si se ha aprobado la información de manera oficial para su emisión al público.

Comentario: El propósito de esta política es recordar a los usuarios que el ambiente informal de Internet no debe dar pie para ignorar las leyes de propiedad intelectual. La informalidad que rodea a Internet ya ha ocasionado numerosos casos de demandas por difamación, los cuales pudieron haberse evitado razonablemente si se hubiese hecho énfasis en esta política. Aunque esta política parezca evidente, puede surgir mucha confusión sobre estos asuntos dentro de la comunidad de usuarios. Es indispensable establecer claramente las expectativas del usuario y, de ser necesario, tener la capacidad para incluir extensivamente referencias sobre el libelo, la calumnia, la difamación y otros problemas legales relacionados.

Políticas Relacionadas:“Validación de Información en Intranet” y “Derechos de Propiedad Intelectual”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

política, debido a que se espera que cambie con el transcurrir del tiempo. Se podrán requerir distintos paquetes de control de acceso para diferentes plataformas de computadores. Igualmente, la política evitará que empleados bien intencionados establezcan conexiones de red que pongan en peligro la seguridad de las redes internas y de los computadores conectados. Por ejemplo, esto podría llevarse a cabo si un usuario deja su trabajo correspondiente para ese día y de manera deliberada, mantuvo encendido su modem con un paquete de comunicaciones habilitado dentro del

computador. Aunque esto le permita trabajar desde su casa, también podría permitir a otros obtener acceso inmediato a los sistemas de la organización. Esta política es básicamente una declaración sobre la estructura de la seguridad en la red, expresada de manera que evite que los usuarios puedan afirmar que no estaban conscientes de dicho requerimiento.

Políticas Relacionadas: “[Interconexión de Sistemas](#)” y “[Control de Acceso a Computadores de Red](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

2. Conexiones a Redes de Terceros

Política: Los computadores o redes de la Empresa X deben conectarse sólo a computadores o redes de terceros después de que la gerencia de Seguridad Informática determine que el sistema combinado satisface los requerimientos de seguridad de la Empresa X.

Comentario: Muchas organizaciones tienen problemas con asuntos de la interconexión de sistemas relativos a la administración descentralizada de los mismos. Por ejemplo, la administración del departamento de Mercadeo podría conectar una red interna local de la Empresa X con la red interna de una empresa de consultoría, sin revisar las consecuencias sobre la seguridad. Para evitar las exposiciones que introducen tales acciones es necesaria una cantidad mínima de centralización. Esta política informa al personal interno que la gerencia de Seguridad Informática sí exige requisitos previos para las conexiones con las redes y sistemas de terceros y que éstos se deben cumplir antes de permitir cualquier conexión. Los requisitos específicos quedan deliberadamente fuera de la política, pero por lo general incluirían una autenticación extendida del usuario, controles de acceso privilegiados y registro de la actividad del usuario. Se espera que los requisitos específicos cambien con el correr del tiempo, mientras que la política no necesita ningún cambio con cada modificación de estos requisitos.

Políticas Relacionadas: “[Sistemas de Terceros Conectados a la Red](#)” e “[Interconexión de Sistemas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Modem de Estaciones de Trabajo

Política: Los trabajadores no deben conectar modem de discado a las estaciones de trabajo, computadores personales o a los clientes de red de área local que estén conectados simultáneamente a otra red de área local o a otra red de comunicación interna.

Comentario: El objetivo de esta política es prohibir a los usuarios establecer un enlace débil en un sistema de controles de acceso a la red. Para poder trabajar en casa, trabajar mientras se encuentra en viaje de negocios y permitir a los demás trabajar en tiempo real con ellos, los usuarios establecen a menudo conexiones del modem de marcaje de números telefónicos a sus terminales, computadores personales o clientes de una red de área local. Desafortunadamente, si el terminal se conecta también a un red interna, esa conexión al modem puede permitir a personas no autorizadas entrar a la red interna. Esto puede ocurrir ocasionalmente, sin contraseñas u otros controles de acceso. Esto puede permitir a las personas no autorizadas acceder a los servicios de intranet, mainframes conectadas y demás sistemas. Si bien esta política parece un tanto estricta, permite a los usuarios desconectarse de la red interna cuando utilizan un modem de discado. Se puede extender esta política para incluir conexiones de Internet en lugar de sólo conexiones con sistemas de discado telefónico. En este caso, no se permitirá a los usuarios conectarse simultáneamente a Internet y a una red interna, a menos que pase por un sistema de cortafuegos aprobado. El software cortafuego podría obligar al cumplimiento de políticas de este tipo. Igualmente, se puede extender la política para incluir comunicaciones de discado analógico y digital, en cuyo caso debe evitarse el término “modem”.

Políticas Relacionadas: “[Autentificación de Usuario Que Accede Vía Teléfonica](#),” “[Conexiones Discadas](#),” “[Cambios en la Línea de Comunicación](#),” y “[Sistemas de Redes Desatendidos](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Conexiones de Discado Directo

Política: Todas las conexiones de discado con sistemas y redes de la Empresa X deben enrutarse a través de un grupo de modem que incluya un sistema de seguridad aprobado de autenticación extendida de usuario.

Comentario: Esta política elimina la vulnerabilidad de seguridad creada por las conexiones con sistemas de discado que entran directamente a los computadores

personales. Para evitar estos tipos de conexiones, ciertas organizaciones darán a los usuarios una configuración normal de hardware de computador sin modem. En esta política, los términos "autentificación extendida de usuario" se refieren a las tarjetas inteligentes portátiles y el sistema de contraseñas dinámicas de solicitud/respuesta. Estos sistemas de autentificación son necesarios para legitimar la identidad de los usuarios de manera definitiva, antes de darles privilegios de entrada a las comunicaciones a través de un sistema de discado. En caso de que no se haya establecido la identidad de los usuarios en forma confiable, no se podrán cumplir los controles de privilegios de manera efectiva. En muchos casos, las restricciones salientes son adecuadas debido a que la información patentada o confidencial puede comunicarse fácilmente a través de líneas de discado. Las organizaciones menos preocupadas por la seguridad desearán modificar la política de modo que restrinja únicamente las conexiones entrantes. Una de las mejores maneras de cumplir esta política es retirar materialmente el modem del hardware de escritorio. Esto se debe a que los usuarios pueden habilitar conexiones de entradas que anteriormente se encontraban inhabilitadas, sencillamente cambiando los parámetros del modem.

Políticas Relacionadas: “Modem de Estaciones de Trabajo” y “Conexiones Discadas”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

5. Registro de Línea de Modem

Política: Los empleados no deben instalar o contratar la instalación de líneas de modem que se conecten a computadores o redes de la Empresa X, a menos que ue estas líneas hayan sido autorizadas por la gerencia del departamento de Telecomunicaciones e ingresadas al registro de líneas de modem de toda la organización.

Comentario: Esta política prohíbe a los usuarios y otros llamar a la empresa telefónica e instalar líneas de modem que se conecten a computadores y redes internos. Esta política informa a los usuarios que deben obtener la aprobación e introducción de esta línea dentro del registro de línea de modem. El personal de seguridad informática puede hacer uso de este registro al realizar ataques de penetración u otros tipos de evaluación de riesgos. Esta política se puede utilizar como fundamento de acciones disciplinarias, por ejemplo, cuando un

empleado instala la conexión de un modem, pero no obtiene la autorización adecuada. La administración del departamento de Comunicaciones no debe aprobar todas las solicitudes sin determinar si la nueva línea de modem pondrá en peligro la seguridad interna del sistema informático. También podrán requerir el uso de sistemas de autentificación extendida de usuario, a fin de asegurar aún más la conexión por discado. Asimismo, la administración debe revisar las cuentas telefónicas y mantener el registro, de modo que esté siempre actualizado. Adicionalmente, el registro podría ser de gran utilidad al investigar delitos cometidos con computadores, debido a que muestra posibles rutas de entrada a la red. Esta política funciona mejor si la organización tiene un sistema telefónico digital, en cuyo caso los modem analógicos no funcionarían en las líneas conectadas a cada oficina.

Políticas Relacionadas: “Conexiones de Discado Directo” y “Sistemas Que Aceptan Llamadas Discadas Entrantes”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

6. Modem en Auto-Respuesta

Política: Los usuarios no deben dejar conectados los modem a los computadores personales en función de respuesta automática, de modo que puedan recibir llamadas discadas entrantes.

Comentario: El propósito de esta política es garantizar que los usuarios no se vayan a casa o de paseo y dejen encendidos sus modem. Si los usuarios lo hacen, exponen a la organización a visitantes no autorizados. Si bien la exposición pudiera ser seria si se utilizara un computador personal (PC) de producción, el problema se torna particularmente grave si el PC se encuentra conectado a una red interna. Esta política depende del hecho de que los usuarios apaguen sus modem, se salgan de su software de comunicaciones o apaguen sus computadores, en lugar de prohibir el uso de modem o inclusive requerir contraseñas dinámicas.

Políticas Relacionadas: “Conexiones Discadas” y “Autentificación de Usuario Que Accede Vía Teléfono”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Bajos y medianos

9.04.03 Autentificación del Usuario para Conexiones Externas

1. Contraseñas de Acceso Remoto

Política: No debe permitirse que identificadores de usuario que presenten contraseñas en blanco o nulas, obtengan acceso remoto a cualquier computador o red de la Empresa X.

Comentario: Esta política aclara que, para todo acceso remoto, se requiere de una contraseña fija seleccionada por el usuario que no presente espacios en blanco ni sea nula. Esto evitará que la gente que conoce simplemente el identificador de usuario obtenga acceso no autorizado. Esta es una política muy básica que cada organización debe poner en marcha; que por lo menos se utilicen las contraseñas fijas para la autentificación de la identidad del usuario para obtener acceso remoto. Al considerar el acceso remoto, se deben sustituir las contraseñas fijas con tecnologías más sólidas, como las contraseñas dinámicas.

Políticas Relacionadas: “[Estructura de las Contraseñas](#)” y “[Longitud Mínima de Contraseñas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Autentificación de Usuario Mediante Dos Factores

Política: Todos los accesos entrantes que se realicen a través de una red pública hasta todos los computadores de la Empresa X deben emplear una autentificación del usuario mediante dos factores, sin someter a repetición al menos a uno de los factores.

Comentario: Esta política requiere que los diseñadores de sistemas implementen la autentificación del usuario mediante dos factores en sistemas de comunicaciones que se conecten a redes públicas. Esta política es notable porque maneja los problemas de repetición que son ignorados ampliamente dentro del campo de seguridad informática. Cualquier contraseña enviada por Internet se puede repetir si puede ser separada del resto de la información, incluso cuando se trata de una contraseña cifrada. Ciertos tipos de cifrados no proporcionan el nivel de seguridad que se está buscando. Esta política requiere ciertos componentes aleatorios, en donde se modifica el texto cifrado cada vez que se envíe el mismo texto legible. El proceso de ingreso al sistema estará inmunizado contra las amenazas de intercepción y repetición posterior sólo cuando se ponga en marcha dicho componente aleatorio. El cifrado de sesiones,

como el cifrado que proporciona una red privada virtual (VPN, por sus siglas en inglés), proporcionará un componente aleatorio. Los productos VPN que se encuentran en el mercado incluirán el cifrado de la sesión y una contraseña fija que pudiera también considerarse una autentificación de dos factores.

Políticas Relacionadas: “[Contraseñas Legibles](#)” y “[Acceso Entrante a Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

3. Controles de Acceso para Sistemas Remotos

Política: Todos los computadores que tengan diálogos remotos en tiempo real con los sistemas de producción de la Empresa X, deben ejecutar un paquete de control de acceso aprobado por la gerencia de Seguridad Informática.

Comentario: Esta política define los computadores que deben tener paquetes especiales de control de acceso. La política reconoce que el procesamiento distribuido relacionado con los sistemas de computación trae consigo la necesidad de asegurar todos los puntos finales que se pudieran utilizar para introducir la información a un sistema de producción. Estos puntos finales pudieran ser computadores móviles, un asistente personal digital o un teléfono inteligente. Para lograr un nivel adecuado de seguridad de los sistemas de producción, esta política requiere que el sistema remoto que tenga acceso a un sistema de producción cuente con un mecanismo aprobado de acceso. Se excluye de manera deliberada en esta política la definición exacta del sistema remoto, de modo que pueda abarcar una amplia variedad de sistemas. Por lo general, las transmisiones por lotes son más seguras y no se encuentran dentro del ámbito de esta política. Para incrementar la cobertura de esta política, se pudieran incluir sistemas por lotes y sistemas en tiempo real. Una de las ventajas que tiene esta política es que los computadores remotos de los usuarios de los sistemas de producción pueden cerrarse con una herramienta de control de cambios que recorre el sistema de control de acceso y evita que los usuarios cambien la configuración del software interno. De manera indirecta, esta política también maneja la descarga de datos y establece paquetes de control de acceso en todos los sistemas remotos que pudieran almacenar información de producción.

Políticas Relacionadas: “Controles de Acceso al Sistema de Computación” y “Procedimientos de Seguridad Informática en Teletrabajo”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Acceso a la Red

Política: Todos los usuarios deben verificar su identidad a través de un identificador de usuario y una contraseña secreta o por otro medio que proporcione una seguridad igual o mayor, antes de permitirse su utilización de los computadores de la Empresa X conectados a una red.

Comentario: El propósito de esta política es garantizar que sólo los usuarios autorizados podrán tener acceso a las redes de la organización. Esta política implica que un grupo de personas podrían compartir una contraseña e identificador de usuario, aun cuando no se debe fomentar este procedimiento, debido a que no proporciona responsabilidad individual. Asimismo, esta política permite a la organización pasar a la autenticación extendida del usuario, a través de la biometría, sistemas de devolución de llamadas, tarjetas portátiles de identidad con contraseñas dinámicas o certificados digitales. Se pudiera redactar esta política de modo que se aplique más bien a sistemas multiusuario en lugar de computadores conectados a una red. Esto significaría que no es aplicable a los computadores personales ni a las estaciones de trabajo. Igualmente, pudiera ser necesario definir dentro de este contexto lo que se tiene entendido por red.

Políticas Relacionadas: “Códigos de Identificación para Soporte Técnico” e “Identificadores de Usuario para Terceros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Administración Remota

Política: La gestión remota de computadores conectados a Internet debe emplear contraseñas que se utilicen una sola vez sobre enlaces cifrados.

Comentario: El objetivo de esta política es garantizar que los intrusos no se aprovecharán de las capacidades de administración remota que se encuentren habilitadas en computadores de la Empresa X conectados a Internet. Estas capacidades son un objetivo atractivo para los intrusos, debido a que, con frecuencia, las capacidades

de administración contienen amplios privilegios. El uso de contraseñas dinámicas que se utilizan una sola vez y los enlaces cifrados ayudan mucho en la restricción de este acceso a las personas autorizadas.

Políticas Relacionadas: “Conexiones a Redes Externas en Tiempo Real,” “Autentificación del Usuario por el Sistema Operativo,” y “Contraseñas para los Dispositivos Internos de la Red”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Comandos Inter-Procesador

Política: No se deben satisfacer los comandos iniciados por usuarios provenientes de zonas externas, a menos que el usuario inicie su sesión.

Comentario: Una de las maneras de obtener acceso no autorizado a sistemas conectados a la red Internet es utilizar el comando “finger”, el cual proporciona información sobre usuarios que puede luego utilizarse para deducir su identificador de usuario y contraseña. Con frecuencia, no es necesario iniciar una sesión para ejecutar este comando. Esta política expresa un objetivo de diseño de sistemas que debe utilizarse al momento de establecer los controles de acceso al sistema y que debe usarse al momento de definir arquitecturas multi-procesador de seguridad. La idea es que los externos no reciban información sobre un sistema hasta tanto no se identifiquen adecuadamente. La política no restringe el uso de llamadas de procedimiento remotas iniciadas por un sistema fuera de la Empresa X.

Políticas Relacionadas: “Información en Mensaje de Inicio de Sesión,” “Autentificación de Usuario Que Accede Vía Teléfono,” y “Autentificación del Usuario por el Sistema Operativo”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Autentificación de Usuario Que Accede Vía Teléfono

Política: Todas las conexiones discadas entrantes con la red de datos de computación de la Empresa X deben utilizar autentificación extendida de usuario.

Comentario: Esta política exige controles adicionales de acceso al sistema para todas las conexiones entrantes con la red telefónica pública. El ámbito de esta política se puede expandir para incluir todas las conexiones de

redes externas, inclusive las conexiones entrantes en Internet. Se exigen los controles de acceso extras, debido a que estos puntos de interacción han sido históricamente vulnerables. Los sistemas de autentificación extendida de usuario son los más utilizados conjuntamente con los identificadores de usuario y contraseñas, aun cuando se pueden también sustituir los identificadores de usuario o contraseñas. A menudo, los sistemas de autentificación extendida del usuario son más costosos, menos beneficiosos para el usuario y más difíciles de administrar, así que se puede modificar esta política de modo que se pueda aplicar solamente a los sistemas de computadores que contienen datos particularmente sensibles. Las organizaciones que cuentan con sistemas extensivamente interconectados encontrarán que es relativamente poco significativa la limitación de esta política a aquellos computadores que tienen este tipo de datos. Una vez que el usuario haya obtenido acceso a la red, podrá establecer conexiones con una amplia variedad de computadores, dependiendo de los controles de flujo dentro de la red interna.

Políticas Relacionadas: “Modem de Estaciones de Trabajo,” “Cambios en la Sensibilidad, Criticidad y Valor de la Información,” “Validación de la Identidad de Terceros,” “Acceso Entrante a Internet,” y “Autentificación del Usuario por el Sistema Operativo”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Intentos de Contraseñas por Discado

Política: Todas las líneas de discado deben configurarse de manera de concluir la conexión con el usuario que no haya proporcionado una contraseña correcta luego de tres intentos consecutivos.

Comentario: Esta política evita que los programas de deducción de contraseñas descubran las contraseñas utilizadas en accesos discados. Con frecuencia, las líneas de discado son la vía mediante la cual los usuarios no autorizados logran obtener el acceso a los sistemas. Sin embargo, este enfoque está exento de inconvenientes. Por ejemplo, los atacantes pueden devolver la llamada de inmediato, pero el proceso para deducir la contraseña tardará más tiempo y es mucho más costoso de lo que sería sin este enfoque. Otra de las propuestas que utilizan las organizaciones que tienen sistemas de control de acceso a la medida, incluye la prolongación progresiva del período de tiempo de cada intento. En este caso, el tiempo entre la solicitud del identificador de usuario y la contraseña para tratar de ingresar al sistema con cierto identificador de usuario podría ser de

un segundo, mientras que entre el segundo y tercer intento puede ser de dos segundos. Este enfoque imposibilita el uso satisfactorio de los programas de deducción de contraseñas para probar numerosas posibilidades. Se puede expandir esta política para que incluya las conexiones en Internet, en cuyo caso todos los usuarios entrantes a Internet tendrían un corte del proceso de inicio de sesión, si no lograran suministrar la contraseña correcta después de una cantidad determinada de intentos. Entonces se puede imponer un retraso entre los intentos de inicio de sesión utilizando el mismo identificador de usuario. Esta política ha sido utilizada históricamente para los sistemas de control de acceso con contraseñas fijas, pero también es aplicable a los sistemas de contraseñas dinámicas.

Políticas Relacionadas: “Configuración de Modem para Llamadas Discadas Entrantes” e “Intentos de Introducir Contraseña”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Acceso Entrante a Internet

Política: Todos los usuarios que establezcan una conexión con los computadores de la Empresa X en su red interna a través de Internet deben autenticarse en un cortafuego que emplee un proceso extendido de autentificación de usuario aprobado por la gerencia de Sistemas Informáticos.

Comentario: Esta política describe una de las funciones principales que debe llevar a cabo un cortafuego efectivo en Internet. Los cortafuegos permiten conexiones salientes sin obstáculo alguno, pero detendrán y pondrán obstáculos importantes a todos aquellos que deseen establecer una conexión entrante a través del cortafuego. Esta política evita de manera deliberada la discusión sobre la tecnología que se va a emplear, en gran parte debido a que se espera que cambie rápidamente en los próximos años. Los sistemas de contraseñas dinámicas se utilizan mayormente en el cortafuego para autenticar la identidad de los usuarios internos. Además de estos sistemas fundamentados en tarjetas inteligentes, se puede utilizar otra tecnología de contraseñas dinámicas, como los sistemas de exigencia/respuesta que son transparentes para el usuario. Igualmente, se puede utilizar cifrado de sesión completa como alternativa a las contraseñas dinámicas.

Políticas Relacionadas: “Conexiones a Internet,” “Contraseñas Legibles,” y “Autentificación de Usuario Que Accede Vía Teléfono”

Política Dirigida a:Personal técnico

9.04.04 Autentificación de Nodos

1. Sistemas Que Aceptan Llamadas Discadas Entrantes

Política: Los empleados de la Empresa X no deben establecer ningún sistema de comunicación que acepte llamadas entrantes discadas, a menos que la gerencia de Seguridad Informática lo haya aprobado.

Comentario: Esta política evita la divulgación inadvertida de información de la Empresa X a personas ajenas a la misma y evita que los empleados establezcan vías no autorizadas e insuficientemente seguras para acceder a las redes de la Empresa X. Dada la amplia disponibilidad de las facilidades de discado, incluso los usuarios finales pueden establecer un servidor o computador de escritorio con ciertas capacidades de discado entrante. Para evitar esto, existe la necesidad de informar a los usuarios que deben obtener la aprobación de tales sistemas accesibles en sistemas de discado. Por ejemplo, esta política prohíbe incluso el acceso temporal al discado nocturno, el cual se establece conectando un modem a una línea de voz analógica. Se puede agregar a esta política una excepción especial y permisible para sistemas de una sola aplicación, tales como las unidades interactivas de respuesta de voz. Se pueden agregar

Ambientes de Seguridad:Todos

otras excepciones, tales como las pruebas de nuevos sistemas que no estén conectados a ninguna red interna o el uso autorizado de puertos de mantenimiento remotos que instale un proveedor. Si bien se pueden mencionar estas excepciones en la política, resulta mejor manejarlas a través de un proceso de excepción conocido y aprobado. Muchos administradores de redes no conocen todos los puntos de acceso a su red. Esta política restringe los puntos de acceso a una cantidad conocida y manejable. La política se puede expandir para incluir las conexiones en Internet, lo cual significaría que se prohibiría el establecimiento de alguna conexión entrante en Internet, salvo que se obtenga la aprobación de la gerencia. Lo ideal es que el proceso de autorización incluya un requisito relativo a la utilización de un sistema de control de acceso aprobado en la conexión.

Políticas Relacionadas:“[Conexiones Discadas](#)” y “[Cambios en la Línea de Comunicación](#)”

Política Dirigida a:Usuarios finales y personal técnico**Ambientes de Seguridad:**Todos

9.04.05 Protección del Puerto Remoto de Diagnóstico

1. Acceso al Puerto de Diagnóstico

Política: El acceso a los puertos de diagnóstico debe controlarse de manera segura con el uso de un bloqueador de teclados y de procedimientos eficaces.

Comentario: Esta política garantiza que ningún punto de entrada diseñado por los ingenieros de mantenimiento de sistema con fines de diagnóstico remoto, no será explotado por personas no autorizadas. Muchos sistemas de computación y de comunicaciones están

diseñados con un puerto dedicado para marcar el número telefónico hacia el sistema. Si se dejan abiertos o sin protección, estos puertos pueden utilizarse para obtener acceso no autorizado al sistema.

Políticas Relacionadas:“[Hardware y Software de Diagnóstico](#)”

Política Dirigida a:Gerencia y personal técnico**Ambientes de Seguridad:**Todos

9.04.06 Segregación en las Redes

1. Conexiones Personales a la Red

Política: Todo acceso personal que permita a los visitantes conectarse con sus propias redes, debe emplear una subred separada que no tenga conexión con

la red interna de la Empresa X.

Comentario: Esta política evita que personas no autorizadas obtengan acceso a los computadores conectados a la red interna y los recursos informáticos

que allí se encuentran. Si una organización proporciona conexiones personales que permitan a los usuarios conectarse rápidamente a través de un computador portátil con la red interna de una organización, aumenta considerablemente el riesgo de sufrir ataques. Para aislar las conexiones personales, pero a la vez proporcionar este servicio de gran utilidad, se podría utilizar una subred separada. Aun cuando no se menciona en esta política, se debe proporcionar también seguridad física en torno a estos puntos de acceso a las redes. Por ejemplo, las áreas de recepción y las salas de conferencia que tengan estos puntos de acceso deben estar cerradas cuando la organización involucrada no esté funcionando.

Políticas Relacionadas: “[Interconexión de Sistemas](#)” y “[Servidores Públicos en Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Computadores y Redes de Alta Seguridad y Alta Confiabilidad

Política: Todo sistema de alta seguridad y de alta confiabilidad manejado o propiedad de la Empresa X debe tener sus propios computadores y redes dedicados, a menos que estén aprobados con antelación por la gerencia de Seguridad Informática.

9.04.07 Control de las Conexiones de la Red

1. Contraseñas para los Dispositivos Internos de la Red

Política: Todas las redes internas de la Empresa X, incluyendo entre otros, enruteadores, cortafuegos y servidores de control de acceso, deben tener contraseñas únicas u otros mecanismos de control de acceso.

Comentario: En un esfuerzo por acelerar la administración, el personal técnico utilizará con frecuencia la misma contraseña para múltiples dispositivos del mismo tipo o incluso para diversos dispositivos. Esta política tiene como fin evitar que el descubrimiento o la divulgación no autorizada de una contraseña fija de red origine un daño extenso. Si se utilizan contraseñas fijas únicas para cada dispositivo, el daño debería restringirse únicamente al dispositivo en cuestión. Si se utiliza la misma contraseña fija en múltiples lugares, será más difícil deshacerse de un hacker. Asimismo, el uso de contraseñas simples para múltiples dispositivos de red

Comentario: El objetivo de esta política es definir claramente la necesidad esencial de todo sistema de alta seguridad y alta confiabilidad que sea propiedad o manejado por la Empresa X. Al utilizarse computadores y redes dedicados, existe considerablemente menos complejidad relacionada con el sistema. Esta simplicidad facilitará el hecho de hacer que el sistema sea seguro y confiable. Asimismo, los sistemas dedicados disminuyen la cantidad de personas y organizaciones asociadas con el sistema y reduce las probabilidades de que existan errores u omisiones, permitiendo a la Empresa X hacer los cambios con mayor rapidez. Ejemplos de sistemas dedicados son las redes de cajeros automáticos. Esta política tiene consecuencias sobre los arreglos de sistemas administrados por terceros y sobre los sistemas administrados internamente.

Políticas Relacionadas: “[Sistemas Comerciales y Financieros en Internet](#)” y “[Aislamiento de Sistemas con Información Secreta](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

restringe la capacidad de la gerencia para establecer la separación de tareas y restringir el acceso con base en las mismas. Adicionalmente, esta política es esencial si se quiere obtener profundidad defensiva en la red. La profundidad defensiva se refiere al establecimiento de múltiples obstáculos a través de los cuales los usuarios deben pasar para poder alcanzar un destino determinado. Estos obstáculos pudieran ser cortafuegos, enruteadores u otros computadores de la red interna. Por ejemplo, la profundidad defensiva se utiliza cuando se utilizan cortafuegos para establecer una zona desmilitarizada en una red interna. Si bien debe desalentarse el uso de "palabras claves" o contraseñas fijas compartidas si la tecnología soporta el uso de otros métodos, la realidad actual en muchas empresas es que se deben emplear contraseñas fijas compartidas. Esta política toca el punto del conflicto que existe entre la facilidad de uso y la seguridad, enfatizando más ésta última.

Políticas Relacionadas: “Identificador Único de Usuario y Contraseña Obligatorios” y “Contraseñas Iniciales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Acceso a Internet Sin Cortafuegos

Política: Todo acceso a Internet sin el uso de un cortafuego debe lograrse a partir de un computador independiente que no esté conectado a ninguna red interna de la Empresa X.

Comentario: Esta política tiene como fin controlar las formas en que se conectan los usuarios a Internet hasta que se pueda instalar un cortafuego adecuado y listo para su operación en producción. Esta política permite a los usuarios acceder a Internet para realizar investigaciones, enviar correos electrónicos y para otros fines. La forma más rápida y fácil de hacer esto es establecer cuentas con los proveedores de servicio en Internet, los cuales pueden prestar estos servicios y establecer una página web independiente de la red interna de la organización. Aunque esta política puede resultar adecuada por un período breve de tiempo, por ejemplo cuando la organización se encuentra estableciendo sus conexiones de red, debe ser pronto sustituida por otra política que exija cortafuegos para todos los computadores conectados a Internet, aunque se utilicen únicamente para conexiones discadas.

Políticas Relacionadas: “Conexiones a Redes Externas en Tiempo Real” y “Conexiones a Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Acceso Público a Puertos Activos de la Red

Política: Los puertos activos de red desatendidos que estén conectados a la red de computadores internos de la Empresa X no deben estar ubicados en áreas públicas que incluyan, entre otros, entradas de edificios, cafeterías de la empresa y salas de conferencia.

Comentario: Esta política evita que los diseñadores de redes, instaladores de cables de red y otros, coloquen puertos activos de datos en lugares donde personas no autorizadas pudieran emplear estos mismos puertos para obtener ingreso no autorizado a los sistemas informáticos internos de la Empresa X. El problema que

se presenta con los puertos activos en áreas públicas es que están a la disposición de cualquier persona y se podrían utilizar para lanzar un ataque de deducción de contraseñas, colocar un virus en los sistemas de computación de la Empresa X, interceptar y grabar de manera pasiva la información que fluya por la red o perpetrar cualquier otra acción abusiva. De acuerdo con esta política, resulta aceptable que estos puertos se encuentren instalados en lugares públicos, pero no deben estar encendidos o activos. Se deberían emplear contraseñas u otros mecanismos de control.

Políticas Relacionadas: “Conexiones Personales a la Red” y “Configuración de Conexiones a la Red”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Puertos de Red en Oficinas Vacías

Política: Todos los puertos de red que se encuentren en oficinas desocupadas y otras áreas normalmente no utilizadas, deben desconectarse rápidamente en el cajetín de instalación o desde otra zona centralizada.

Comentario: La intención de esta política se deriva de la comprensión de un método común de ataque utilizado por espías industriales e intrusos de los sistemas de computadores. Este enfoque tiene que ver con el uso de los puertos de red que se encuentran en las oficinas vacías, salas de conferencia u otras instalaciones desatendidas. Los intrusos pueden utilizar estos puertos para obtener acceso a una red interna y, desde allí, lanzar un ataque en contra de los computadores internos de la Empresa X o, tal vez, contra computadores externos. Esta política informa a los técnicos de redes y otras personas que manejan la infraestructura material de una red interna, que es necesario inhabilitar todos los puertos de red no utilizados desde una ubicación central. No es suficiente inhabilitar el puerto de una ubicación remota, porque el intruso puede reestablecer la conexión fácilmente, con herramientas fácilmente disponibles, como un destornillador. Esta política supone que los cajetines telefónicos y otras ubicaciones de instalación centralizada se encuentran físicamente protegidos o asegurados.

Políticas Relacionadas: “Conexiones Personales a la Red” y “Modem de Estaciones de Trabajo”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

5. Inabilitación de Java

Política: Todos los usuarios de Internet deben inhabilitar los programas Java, modificando la configuración predeterminada de su explorador de Internet.

Comentario: Aunque muchas de las amenazas de subprogramas no autorizados de Java se han generado más en los laboratorios de investigación que en el mundo real, existe un riesgo significativo de que se pudiera utilizar el lenguaje de programación Java para evitar los mecanismos existentes de control de acceso. El daño resultante sería muy similar al de un virus de computador. Aunque muchos cortafuegos pueden filtrar

subprogramas Java, no existen dichos cortafuegos en muchas organizaciones. Es posible que esta política genere una resistencia significativa por parte de los usuarios, debido a que las capacidades que proporciona el lenguaje Java son poderosas y de gran utilidad para muchos usuarios. Esta política podría modificarse para referirse a otros productos de contenido activo.

Políticas Relacionadas: “[Descarga de Software](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

9.04.08 Control de Ruta de la Red

1. Zonas de Seguridad de la Red

Política: Todas las redes internas de datos de la Empresa X deben estar divididas en zonas de seguridad.

Comentario: La presente política adopta un modelo de zonas para la seguridad de la red. Este enfoque ha sido implantado en muchas organizaciones, entre ellas grandes empresas multinacionales y diversas organizaciones militares. En la mayoría de los casos, las definiciones de estas zonas son un tanto parecidas a la siguiente descripción: los computadores de la Zona Roja están expuestas a redes externas, como Internet, y ninguna de ellas deben estar en esta zona, salvo que exista una razón que obligue a ubicarla en la misma. El cortafuego o enrutador protege a los computadores de la Zona Amarilla, de modo que sólo los servicios que sean necesarios queden expuestos a una red externa. Los

computadores de la Zona Verde son accesibles a los de la Zona Amarilla o Zona Azul, mas no a los de la Zona Roja. Las máquinas de la Zona Verde contienen únicamente datos que sirven de soporte a los procesos de negocios y aplicaciones que no pueden ubicarse con seguridad dentro de la Zona Azul. Los computadores de la Zona Azul se encuentran dentro del dominio de la arquitectura de seguridad de la Empresa X, y se debe verificar y revisar toda información enviada desde otras zonas antes de utilizarla.

Políticas Relacionadas: “[Aislamiento de Equipos](#)” y “[Distintas Zonas de Riesgo de Incendio](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9.04.09 Seguridad de los Servicios de la Red

1. Cortafuegos de Servidores Web

Política: Todos los servidores web accesibles desde Internet deben estar protegidos por un enrutador o cortafuego autorizado por el departamento de Seguridad Informática.

Comentario: La colocación de un servidor web dentro de un cortafuego aumenta significativamente la protección frente a los daños que pudiera ocasionar un hacker. Entre los escenarios comunes figuran la inclusión de material desconcertante u ofensivo, ataques de negación del servicio o el uso del servidor para irrumpir en otros sistemas. El servidor web instalado detrás de un

cortafuego reduce las vías que pueden utilizar los hackers para penetrar el sistema. Asimismo, un servidor web facilita el mantenimiento. Deben existir otros cortafuegos entre el servidor web y cualquier computador de producción de la red interna.

Políticas Relacionadas: “[Contraseñas para los Dispositivos Internos de la Red](#)” y “[Acceso a Internet Sin Cortafuegos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9.05 Control de Acceso al Sistema Operativo

9.05.01 Identificación Automática del Terminal

1. Seguridad Física del Terminal

Política: El acceso físico al terminal debe estar restringido a aquellos empleados que necesitan conocer la información, cuando se utilice la identificación del terminal para autenticar la conexión de un terminal a un área específica.

Comentario: El propósito de esta política es establecer controles sobre el uso de terminales que ingresan al sistema de un computador de manera automática, cuando se inicia el sistema o cuando se enciende el terminal y pasa a sistema activo. Estos terminales se encuentran con frecuencia en ambientes donde múltiples usuarios deben acceder a un solo terminal y es necesario tener acceso a la información contenida en el sistema para garantizar un flujo ininterrumpido de productos o servicios. Por ejemplo, estos terminales pueden

encontrarse en la línea de ensamblaje de una fábrica. La clave para utilizar este tipo de terminal es la restricción del acceso físico al dispositivo. Esto es muy importante no sólo para garantizar que la información no quede comprometida, sino también para mantener la seguridad de las personas en ciertas áreas. El uso de estos terminales sacrificará la responsabilidad por las entradas, y debe tomarse en cuenta el establecimiento de controles de compensación, quizás en las aplicaciones utilizadas, para garantizar que la identidad del usuario sea captada en todas las operaciones de ingreso de datos.

Políticas Relacionadas: “Cierre de Sesión Automático”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

9.05.02 Procedimientos para Inicio de Sesión en Terminales

1. Intentos de Introducir Contraseña

Política: Luego de tres intentos infructuosos por introducir su contraseña, la identidad del usuario correspondiente debe quedar suspendida hasta que un administrador de sistemas la reinicialice, desactivada momentáneamente por lo menos durante tres minutos, o desconectada si se utilizan conexiones discadas o externas.

Comentario: Uno de los métodos de ataque más exitoso para lograr acceso al sistema es la deducción de contraseñas. Además de deducir información sensible por el contexto, los atacantes podrían utilizar programas para descubrir contraseñas que revisan todas las palabras del diccionario. Esta política ayudará a garantizar que el ataque será infructuoso, bien sea un ataque manual determinado o un ataque mediante la deducción automatizada de la contraseña. Ciertas organizaciones querrán establecer un período de tiempo a esta política, de modo que las palabras "luego de tres intentos infructuosos" se conviertan en "luego de tres intentos infructuosos en cinco minutos". Un resultado parecido se puede lograr al calificar la misma frase con las palabras "durante una sola sesión". Con esta propuesta, ciertos usuarios legítimos tendrían bloqueados sus identidades si escriben mal, si están aprendiendo a utilizar el sistema o si tienen problemas

para recordar su contraseña. Estos usuarios se comunicarán con el administrador de seguridad para obtener una contraseña vencida nueva. La comunicación con el administrador de seguridad brinda a éste la oportunidad de dar al usuario involucrado la información necesaria para ingresar adecuadamente al sistema, la próxima vez que lo utilice. No hay nada especial en cuanto al número tres. Para dar soporte a un ambiente menos seguro, este número podría ser sencillamente un 5 o un 10. Esta es una de las numerosas políticas dirigidas a los administradores de sistemas en el sentido de cómo deben configurar los sistemas que administran.

Políticas Relacionadas: “Sospecha de Divulgación de Contraseña,” “Contraseñas Iniciales,” “Estructura de las Contraseñas,” e “Intentos de Contraseñas por Discado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Protección de la Reinicialización Basada en Contraseña

Política: Todos los estaciones de trabajo, incluyendo entre otros los computadores personales, computadores portátiles, computadores transportables y computadores

de conexión inalámbrica, deben emplear un sistema de control de acceso aprobado por la gerencia de Seguridad Informática.

Comentario: El propósito de esta política es evitar que personas no autorizadas obtengan acceso a las estaciones de trabajo y a la información sensible que pudiera estar guardada en las mismas. Debido a que, por lo general, estos computadores cuentan con mecanismos de almacenamiento, como el disco duro, también pueden contener información sensible. Al proteger cada uno de los computadores, la gerencia de Seguridad Informática elimina cualquier disputa sobre quién debería utilizar los sistemas de control de acceso de la estación de trabajo. Los paquetes de control de acceso con base en protectores de pantalla son fácilmente derrotables. La aprobación requerida de la gerencia de Seguridad Informática por la presente política significa que sólo se emplearán productos sólidos de protección de pantalla. La información distribuida en el computador de escritorio significa que el control de acceso distribuido es igualmente necesario. Podría ser necesario emitir una norma acerca de la cantidad de minutos antes de invocar al protector de pantalla, lo cual también se puede especificar en esta política.

Políticas Relacionadas: “[Sistemas de Cifrado de Propósito General](#)” y “[Sesiones Activas Desatendidas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Información de Inicio de Sesión

Política: Si alguna parte de la secuencia de inicio de sesión es incorrecta al momento de ingresar al sistema de computación o comunicaciones de datos de la Empresa X, el usuario debe únicamente recibir información de que todo el proceso de inicio de sesión fue incorrecto.

Comentario: Las personas que intenten irrumpir en los sistemas podrían utilizar mensajes específicos de información que determine qué es lo que están haciendo bien. Esto aumenta la probabilidad de que tengan éxito los ataques al sistema. Por ejemplo, si un mensaje indica “contraseña incorrecta”, esto podría ser de gran ayuda, debido a que ya sabe que la identidad del usuario era aceptable. Para evitar que estos ataques sean exitosos, esta política prohíbe el suministro de información detallada a los usuarios. Esto resulta ligeramente poco beneficioso para los usuarios, pero compensa en seguridad la falta de amabilidad que obtiene el usuario en la mayoría de los ambientes. El hecho de propor-

cionar información específica sólo después de introducir toda la información significa que no se puede utilizar el tiempo de duración del mensaje informativo para deducir cuál parte del ingreso al sistema era la incorrecta. Esta política puede modificarse, de modo de no dar a los usuarios ninguna información, cambiando la palabra “específico” por “cualquier”.

Políticas Relacionadas: “[Respuesta por Inicio Incorrecto de Sesión](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Respuesta por Inicio Incorrecto de Sesión

Política: Si alguna parte de la secuencia de inicio de sesión resulta incorrecta al momento de entrar al sistema de computación o de comunicaciones de datos de la Empresa X, el sistema debe dar por terminada la sesión o esperar hasta recibir la información correcta de inicio de sesión.

Comentario: Esta política no proporciona ninguna información que pudieran utilizar las personas que traten de obtener acceso no autorizado al sistema. En ciertas circunstancias, el hecho de que se esperaba una secuencia de inicio de sesión podría ser en sí una divulgación que serviría de ayuda a los atacantes. Esta política no es amigable para el usuario y normalmente se encuentran solamente en ambientes de alta seguridad, como el del sector militar. Naturalmente, esta política sirve de acompañamiento a una política similar que prohíbe los mensajes de bienvenida que pudieran utilizarse para identificar un sistema, una organización o, de algún otro modo, suministrar información que sirva a un atacante del sistema.

Políticas Relacionadas: “[Información de Inicio de Sesión](#)” e “[Información en Mensaje de Inicio de Sesión](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Alto

5. Mensaje de Advertencia en Inicio de Sesión

Política: Toda pantalla de ingreso de los computadores multiusuario debe incluir un aviso especial que indique que sólo los usuarios autorizados pueden acceder al sistema, lo cual significa que los usuarios que ingresan al sistema están autorizados para hacerlo, y que el uso

no autorizado o abuso del sistema está sujeto a enjuiciamiento criminal y que se revisará y registrará el uso del sistema.

Comentario: En muchas jurisdicciones y por razones legales, lo recomendable es notificar a todos los usuarios que el sistema involucrado puede utilizarse únicamente con fines autorizados. En caso de producirse un enjuiciamiento contra aquellas personas que hayan ingresado ilegalmente al sistema, una de los alegatos más exitosos de la parte demandada es que no había ningún aviso que indicara que no podían ingresar al sistema. Los hackers pueden aferrarse a los mensajes de bienvenida que hasta incluyen la palabra "bienvenido". Casos recientes en los tribunales han resaltado la necesidad que tienen las organizaciones de informar a los usuarios no autorizados que estos sistemas están fuera de su alcance. Como resultado, el mensaje de bienvenida que se muestra en las pantallas iniciales debe ser equivalente a una advertencia de no pasar. Algunas organizaciones incluso van más allá, indicando que se trata de un sistema privado y no público y que defenderán su utilización desde tal punto de vista. La política indica a los usuarios que la gerencia mira la seguridad y la privacidad con estricta seriedad. También una política como ésta es deseable para todos los computadores multiusuario, especialmente aquéllos con conexiones externas de red. El mismo tipo de aviso puede utilizarse para ciertas redes de comunicaciones de datos y no sólo los computadores.

Políticas Relacionadas: ["Información en Mensaje de Inicio de Sesión"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Información en Mensaje de Inicio de Sesión

Política: Todos los mensajes de bienvenida de los sistemas de computador de la Empresa X que estén conectados a una red deben guiar al usuario para iniciar su sesión en el sistema y no deben suministrar ninguna información que identifique a la empresa, el sistema operativo, la configuración del sistema u otros asuntos internos hasta que se autentifique exitosamente la identidad del usuario.

Comentario: La falta de información específica, como el nombre de la organización, servirá para que personas no autorizadas no se enteren de nada sobre el sistema alcanzado. Esto haría el sistema menos interesante para ellos, y les daría menos información a utilizar en un

ataque por deducción de contraseñas o por ingeniería social. Asimismo, la falta de información sobre el sistema operativo de un computador evitará que los usuarios empleen el conocimiento de debilidades especializadas de dichos sistemas operativos. Esta política de divulgación de mensajes de bienvenida se fundamenta en la necesidad de conocer la información. Esta política resulta indefinida en cuanto a los pasos necesarios para demostrar su propia identidad, de modo que no sea necesario ningún cambio en la política cuando la organización pase de identificadores de usuario y contraseñas fijas a una tecnología más sofisticada. Esta política podría restringirse a sistemas de red accesibles desde redes externas, tales como Internet y líneas discadas.

Políticas Relacionadas: ["Estructura de las Contraseñas,"](#) ["Comandos Inter-Procesador,"](#) y ["Respuesta por Inicio Incorrecto de Sesión"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Mensaje de Inicio de Sesión en la Red

Política: Se debe utilizar el mensaje normal de advertencia desarrollado por la gerencia de Tecnología Informática y aprobado por el departamento Legal, cuando los usuarios se conecten a los computadores internos de la Empresa X.

Comentario: Esta política informa al personal técnico de sistemas que se debe utilizar un texto específico en todos los mensajes de bienvenida de la red de computadores. Un ejemplo de mensaje de bienvenida es "Este sistema es para uso único de usuarios autorizados. Las personas que utilicen este sistema sin autoridad o con exceso de la misma, están sujetos a que todas sus actividades sean revisadas y registradas por el personal del departamento de sistemas. Durante el transcurso de monitoreo de individuos que estén utilizando el sistema incorrectamente, o en el transcurso de mantenimiento del sistema, también podrían monitorearse las actividades de los usuarios autorizados. Cualquier persona que utilice este sistema aprueba dicha revisión de manera expresa y se le aconseja que en caso de que dicha revisión revele alguna posible actividad delictual, el personal del departamento de Sistemas podrá suministrar pruebas de dicha revisión a las autoridades competentes". Esta política es adecuada para conexiones discadas, conexiones a través de redes de valor agregado y conexiones en Internet. Cada organización podrá modificar los términos para ajustarse a las políticas

establecidas. Es posible que departamentos distintos al de Tecnología Informática y Legal necesiten revisar el contenido de los mensajes de bienvenida.

Políticas Relacionadas: ‘‘Mensaje de Advertencia en Inicio de Sesión,’’ ‘‘Información en Mensaje de Inicio de Sesión,’’ ‘‘Herramientas de Monitoreo de Sistemas,’’ y ‘‘Conexiones Discadas’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Ultima Hora y Fecha de Inicio de Sesión

Política: Al momento de iniciar su sesión, todo usuario debe recibir información que refleje la hora y fecha del último ingreso al sistema.

Comentario: Esta política proporciona al usuario final la información necesaria para determinar si una persona no autorizada utilizó su identificador de usuario. Aun cuando esta política ha sido escrita para el personal técnico, podría aplicarse extensamente a los usuarios finales. Si esto se hiciere, se agregarían palabras que exigirían al usuario recordar la última vez que utilizó el sistema, y luego exigir que el usuario determine si ha habido actividad no autorizada. Ciertos sistemas operativos proporcionan capacidades de este tipo. En otras plataformas podría ser necesario un software adicional que brinde soporte a esa función. Esta política funciona mejor si viene acompañada de otra política que exija el reporte de sospechas de problemas y violaciones a la seguridad informática.

Políticas Relacionadas: ‘‘Informes de Incidentes’’ y ‘‘Privilegios de Identificadores de Usuarios Inactivos’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Límite al Acceso Diario

Política: No se debe permitir a los usuarios ingresar al sistema más de diez veces al día.

Comentario: Esta política detecta y, hasta cierto grado, evita el uso no autorizado del sistema. Si se producen más de diez ingresos al sistema con un identificador de usuario particular en un solo día, esta situación podría indicar la existencia de una distribución no autorizada de contraseñas. No hay nada especial respecto del número diez que se menciona en esta política, ya que podría ser sencillamente un 5 u otro número suficientemente elevado para evitar que los usuarios autorizados se topen con éste normalmente. El propósito es limitar la cantidad de ingresos y generar cierto tipo de informe de ingresos excesivos, de modo que se puedan investigar. Por lo general, este control se aplica más a clientes que a usuarios internos, como los empleados de una empresa. Cuando la cantidad de ingresos supera cierto límite, se puede generar una entrada en el registro.

Políticas Relacionadas: ‘‘Contraseñas Compartidas,’’ ‘‘Ultima Hora y Fecha de Inicio de Sesión,’’ y ‘‘Sesiones Múltiples Simultáneas’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Bajos y medianos

9.05.03 Identificación y Autentificación del Usuario

1. Mecanismo Unico de Acceso

Política: Se debe exigir a los usuarios una sola combinación de identificador de usuario y contraseña, para el momento en que lleguen a la red o al sistema de computadores de destino, luego de lo cual se debe pasar la información relacionada con la identidad del usuario a otros computadores, cortafuegos, sistema de administración de base de datos, sistemas de aplicaciones y demás componente del sistema informático.

Comentario: Como objetivo del diseño de sistemas, ciertas organizaciones tratan de disminuir la cantidad de veces que requieren los usuarios para introducir su identificador de usuario y contraseña que los acredite. En organizaciones con muchos computadores, este

proceso de inicio de sesión puede resultar muy complejo y consumir mucho tiempo. Esta política establece que los usuarios se identificarán una sola vez, como respuesta a las exigencias de interfaces más sencillas por parte del usuario. El proceso transmitirá la identidad del usuario al computador de destino en forma automática. Podría ser necesario hacer una excepción a la propuesta de acceso único, en caso de que un usuario tenga acceso a privilegios especiales o múltiples identificadores de usuario. En este caso, se podría requerir las contraseñas múltiples para controlar los privilegios de acceso y registrar la actividad. Esta propuesta de acceso único está siendo incorporada a los computadores frontales de seguridad que sirven de puerta de enlace y a través de los cuales deben pasar todos los usuarios.

Asimismo, este enfoque resulta posiblemente más económico, debido a que los procesos rigurosos de identificación del usuario, tales como los que incluyen tarjetas inteligentes, requieren aplicarse únicamente al computador frontal. Esta política podría incluir la noción de que la suspensión o revocación del identificador de usuario se realice de manera inmediata y automática en los múltiples computadores de la red. Igualmente, esta política podría formar parte de la arquitectura de seguridad de los sistemas internos.

Políticas Relacionadas: “Protección de la Información” y “Conexiones Discadas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Credenciales Portátiles de Identificación

Política: Las credenciales portátiles de identificación que incluyan o funcionen con computadores, entre ellas las tarjetas inteligentes, las tarjetas portátiles de identidad y los distintivos con foto y barras magnéticas, deben requerir el suministro de una contraseña para funcionar cada vez que se empleen, quedando inhabilitadas de manera automática si los usuarios experimentan tres intentos incorrectos consecutivos para introducir la misma contraseña.

Comentario: Esta política especifica un requerimiento de diseño de sistemas, de modo que el personal del departamento de Sistemas Informáticos que diseñe o integre cualquier tipo de sistema de credenciales, seleccione de manera consistente sólo aquellos proveedores que ofrecen una tecnología especialmente segura. Si no se requiere que la contraseña habilite a la credencial, cualquier persona que robase o incluso encontrase una credencial perdida podría utilizarla para cometer fraude de identidad, obtener acceso a la información confidencial o dañar los sistemas informáticos correspondientes. El límite existente en los intentos incorrectos de introducir la contraseña evita que personas no autorizadas puedan utilizar una credencial perdida o robada, incluso si el usuario autorizado no se ha percatado aún de que perdió la credencial o no ha notificado al administrador de sistemas que la credencial debe quedar inhabilitada. La política soporta la autentificación de dos factores, específicamente algo que sepa el usuario (la contraseña) y algo que posea el usuario (una credencial portátil). Esta política no se aplica a los distintivos con foto que no puedan leerse automáticamente, los pasaportes tradicionales de papel y demás credenciales que no incluyan alguna interfaz de computador.

Políticas Relacionadas: “Proximidad de Contraseñas a Dispositivos de Acceso” y “Distintivos de Acceso Extraviados”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Alto

3. Autentificación del Usuario por el Sistema Operativo

Política: Los desarrolladores de sistemas de aplicación para la Empresa X deben depender consistentemente de los controles de acceso que proporcionan los sistemas operativos, los sistemas de control de acceso disponibles a nivel comercial que mejoran los sistemas operativos, las puertas de enlace o cortafuegos, y no deben crear otros mecanismos para recopilar información, o crear o instalar otros mecanismos de control de acceso que acrediten o autentifiquen la identidad de los usuarios sin el permiso previo de la gerencia de Seguridad Informática.

Comentario: Esta política logra controles de acceso consistentes en todos los sistemas de aplicaciones. En líneas generales, los sistemas operativos, los paquetes relacionados con el control de acceso, las puertas de enlace o los cortafuegos tienen los mecanismos de control de acceso más sólidos de cualquier tipo de software. Por lo general, estos cuatro sistemas proporcionan también facilidades que les permite ser designados mediante aplicaciones, sistemas de administración de base de datos y otros tipos de software. Esta política no sólo hará más fácil y menos costoso el diseño de los sistemas de aplicación, sino que también lo hará más consistente en toda la organización y, en consecuencia, más fácil de manejar. Además, esta política elimina la duplicación de las actividades de la gestión de seguridad. Esta política es plenamente consistente con la generación más reciente de paquetes de gestión de seguridad empresarial que integran todas las actividades administrativas de control de acceso. Esta política se convierte en esencial, cuando la organización intenta establecer una interface consistente para el usuario e interfaces para la programación de aplicaciones consistentes para todas las plataformas de la empresa. Esta política es plenamente consistente con los sistemas de acceso único que pasarán la información de autentificación a los computadores de destino u otro software. Es buena idea que los desarrolladores de aplicaciones se aparten del desarrollo o mantenimiento de los sistemas de control de acceso, ya que limita los caballos de Troya y rutas de acceso no autorizadas que ellos pudieran establecer. Eso significa también que el sistema de control de acceso no tiene que ser verificado

nuevamente cada vez que se efectúen los cambios al código de la aplicación. Asimismo, esta política resulta importante para ambientes de sistemas pequeños donde los usuarios finales diseñan sus propios sistemas de aplicación.

Políticas Relacionadas: “Mecanismo Único de Acceso,” “Regulación del Software,” y “Burlado de los Controles de Acceso”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Sesiones Múltiples Simultáneas

Política: Los sistemas de computación no deben permitir que ningún usuario realice sesiones múltiples simultáneas en línea, a menos que la gerencia de Sistemas Informáticos otorgue un permiso especial.

Comentario: Apenas un porcentaje muy pequeño de usuarios requieren de sesiones múltiples simultáneas en línea. Estas sesiones indican a menudo el uso no autorizado, tal como ocurre con un grupo de hackers que utilizan el mismo identificador de usuario. Los registros de la actividad del sistema y el software de control de acceso podrían alertar al personal de operaciones computarizadas o de seguridad computarizada sobre la existencia de dichas sesiones. Si se prohíbe a los usuarios tener sesiones múltiples simultáneas, este software podrá hacer su trabajo sin tener que notificar a los operadores de computadores, administradores de seguridad y usuarios. En algunos casos, la necesidad de sesiones múltiples simultáneas es un reflejo de privilegios asignados inadecuadamente. Esta política podría requerir una reevaluación de los privilegios, donde corresponda.

Políticas Relacionadas: “Privilegios Especiales en Sistema”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Iniciación de Transacciones en Computadores

Política: La capacidad para ejecutar las transacciones a nombre de la Empresa X debe restringirse mediante los identificadores de usuario individuales y la identificación positiva de las personas involucradas que utilicen dichos identificadores de usuario.

Comentario: Esta política evita que personas no autorizadas puedan iniciar transacciones comerciales vinculantes a nombre de la Empresa X. Un ejemplo de dicha transacción comercial incluye la instrucción que da un banco para efectuar una transferencia electrónica preparada utilizando los sistemas de la Empresa X. Para llegar a este punto, se acostumbra requerir que los usuarios autorizados suministren sus identificadores de usuario y una contraseña secreta. Esta política está redactada de tal modo que las contraseñas no sean la única manera de lograr una identificación positiva. Por ejemplo, se podría lograr el mismo objetivo con las tarjetas inteligentes, tarjetas portátiles de identidad, lectores de huellas dactilares o certificados digitales. Es obligatoria la identificación positiva de los usuarios para poder obligar a la separación de responsabilidades dentro de un ambiente computarizado. Para que esto sea efectivo, es posible que sea necesario agregar la definición de "transacción comercial" a esta política. La noción de "sistemas de producción de negocios" puede resultar una idea útil en la preparación de esta definición.

Políticas Relacionadas: “Separación de Tareas”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Códigos de Identificación para Soporte Técnico

Política: La identidad de las personas que realicen llamadas telefónicas para solicitar soporte computarizado deben quedar autenticadas a través de un código especial de identificación, distinto al de la contraseña de computador y divulgado únicamente al personal interno autorizado, a menos que se reconozca de manera definitiva la voz de la persona que está realizando la llamada.

Comentario: Esta política impide la ingeniería social o el hacerse pasar por una persona autorizada. Los espías industriales, los hackers de sistemas y otros, utilizan con frecuencia la ingeniería social en su esfuerzo por obtener los números de un empleado, sus números telefónicos, direcciones, contraseñas y otra información que pueda ser útil para acceder a computadores y redes. Las contraseñas de los computadores no son la forma adecuada para autenticar la identidad de cada trabajador ante el personal de soporte computarizado, porque la contraseña debe conocerla únicamente la persona que está relacionada a ésta. Asimismo, los números de empleado, números de seguro social, u otros números específicos de cada empleado que puedan obtenerse de inmediato no deben ser formas definitivas

para autenticar la identidad del personal interno. Los códigos de identificación para soporte computarizado deben estar únicamente a la disposición de aquellos miembros del personal que tengan una necesidad justificada de conocer la información. En algunas organizaciones, la utilización de códigos de identificación puede expandirse para incluir la liberación por teléfono de información sensible, como el salario y los beneficios laborales. Puede necesitarse el cambio de la

cultura corporativa de tal manera de hacer frecuente el uso de tales códigos, a menos que el telefonista se abstenga de solicitar el código por razones de cortesía.

Políticas Relacionadas: “Contraseñas de Control de Acceso al Sistema” y “Ordenes para Cambiar Registros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9.05.04 Sistema de Manejo de Contraseñas

1. Longitud Mínima de Contraseñas

Política: Todas las contraseñas deben tener por lo menos 10 caracteres y esta longitud debe revisarse siempre de manera automática al momento en que los usuarios crean y seleccionan sus contraseñas.

Comentario: Las contraseñas fijas constituyen la única línea de defensa en muchos sistemas. La deducción de contraseñas fijas sigue siendo un método de ataque que resulta, con frecuencia, exitoso para que personas no autorizadas obtengan acceso al sistema. La deducción de contraseñas se realiza con mayor frecuencia con herramientas automatizadas como programas de ataque mediante diccionarios. Las contraseñas que tienen apenas unos pocos caracteres son más fáciles de deducir que las contraseñas que tienen por lo menos 10 caracteres. Según los expertos, se considera adecuada la extensión mínima de una contraseña de diez caracteres. Esta política podría extenderse con requisitos adicionales, tales como la prohibición de repetir caracteres en una contraseña. Esta política se aplica a contraseñas seleccionadas por el usuario y contraseñas generadas por el sistema. Por esta razón, se utilizaron en esta política las palabras “crear y seleccionar”. En la mayoría de las plataformas, se puede utilizar el software del sistema operativo o el software de seguridad en el control de acceso enlazado, para hacer cumplir esta política de manera automática. Esta política podría restringirse al sistema y a las contraseñas de control de acceso en la red, a fin de permitir que los sistemas de administración de base de datos, programas de aplicación y sistemas de correo de voz utilicen menos caracteres en una contraseña.

Políticas Relacionadas: “Identificadores de Usuarios Anónimos,” “Intentos de Introducir Contraseña,” “Intentos de Contraseñas por Discado,” “Información en Mensaje de Inicio de Sesión,” y “Contraseñas en Distintos Sistemas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Restricción a la Longitud Mínima de las Contraseñas

Política: Las contraseñas fijas seleccionadas por el usuario deben tener una longitud de por lo menos 10 caracteres o la extensión máxima que permita el sistema.

Comentario: Las contraseñas fijas, tal vez el mecanismo de control de computación más conocido, son utilizadas ampliamente, aun cuando hayan demostrado ser susceptibles a la intercepción cuando son transmitidas y a la deducción de personas que tienen cierto conocimiento sobre el usuario. El número máximo de caracteres en una contraseña de ciertos sistemas podría limitarse a seis, siete u ocho, en cuyo caso, no es posible aplicar una política que especifique una extensión mínima de 10 caracteres en una contraseña. Esta política reconoce esta restricción, pero requiere que todos los sistemas que puedan soportar una contraseña de 10 caracteres queden fijos en dicha longitud. El requisito de extensión de una contraseña es una forma de compensar las deficiencias que presentan las contraseñas fijas. Mientras más extensa es una contraseña, más difícil será deducirla y menos probable es que sucumba a los diversos ataques automatizados, tales como ataques mediante diccionarios.

Políticas Relacionadas: “Longitud Mínima de Contraseñas” y “Acceso Entrante a Internet”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Contraseñas para Computadores Conectados a la Red

Política: Todos los computadores conectados a la red de la Empresa X deben emplear contraseñas fijas que contengan al menos 10 caracteres y todos los computadores que no estén conectados a la red deben emplear contraseñas fijas que contengan al menos 6 caracteres.

Comentario: Esta política garantiza que los computadores conectados a la red se encuentran protegidos con una norma superior a las de aquellos computadores que no lo están. Los computadores conectados a la red requieren de un mayor nivel de seguridad, debido a que las personas no autorizadas pueden tener acceso inmediato a ellos. A menudo, las contraseñas fijas de los computadores conectados a la red no proporcionan suficiente seguridad. Podrían requerirse contraseñas dinámicas, diálogos de exigencia/respuesta, biometría u otras tecnologías de autenticación extendida de usuario. Esta política difiere de las políticas tradicionales sobre la extensión mínima de las contraseñas fijas, en el sentido de que reconoce el hecho de que los computadores conectados a la red requieren de una seguridad significativamente mayor. Las políticas tradicionales sobre la extensión mínima de las contraseñas no hacen tal distinción. Los computadores conectados a Internet requieren de una mayor seguridad que los computadores conectados a redes internas. Esto se debe a que la cantidad de personas desconocidas y poco confiables es mucho mayor en Internet que en una red interna.

Políticas Relacionadas: “[Información en Mensaje de Inicio de Sesión](#)” y “[Múltiples Identificadores de Usuario](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Longitud de Contraseña de Acuerdo con la Función

Política: Se debe establecer la longitud mínima de contraseñas fijas a seis caracteres para las casillas del correo de voz y computadores inalámbricos, ocho para todos los computadores conectados a una red y diez para administradores y otros identificadores de usuarios privilegiados.

Comentario: Esta política crea distintos grupos de contraseñas fijas que tienen sus propios requerimientos de extensión mínima. Los requerimientos que se especifican en esta política, guían a los administradores de sistemas en la configuración de los computadores y

redes. Los productos que se encuentran actualmente en el mercado convierten las políticas de este tipo en reglamentos exigibles para el control de acceso. No hay nada de especial en torno al uso de tres categorías, ya que la empresa pudo haber seleccionado cinco categorías fácilmente, en caso de que sean requeridas. Asimismo, no hay nada de especial respecto al uso de un mínimo de seis, ocho o diez, ya que este número pudo haber sido cinco, diez y quince. La idea fundamental de las extensiones mínimas es utilizar controles más estrictos, sólo en los casos en que éstos sean necesarios. Esta política refleja una evolución de pensamiento en torno a los requisitos de longitud de las contraseñas fijas. No se deben aplicar requisitos de una sola longitud a todos los sistemas de toda una organización. Esta política supone que los usuarios han recibido instrucciones de no manejar información sensible a través del correo de voz o computadores inalámbricos.

Políticas Relacionadas: “[Credenciales Portátiles de Identificación](#)” y “[Contraseñas Generadas por el Sistema](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

5. Reutilización de Contraseñas

Política: Los usuarios no deben crear contraseñas que sean idénticas o sustancialmente parecidas a las contraseñas que habían empleado anteriormente.

Comentario: Esta política evita que los usuarios reciclen las contraseñas que habían empleado anteriormente. Por ejemplo, ciertos sistemas operativos evitarán que los usuarios empleen alguna de las últimas quince contraseñas. El usuario podría tener un listado de 16 contraseñas que se generan mediante una regla empírica y utilizar estas mismas contraseñas una y otra vez. En los demás sistemas operativos, sólo una contraseña está registrada, de modo que el usuario pueda alternarse entre las dos contraseñas. El uso repetido de contraseñas aumenta las posibilidades de que una contraseña sea divulgada a personas no autorizadas y éstas aprovechen la información. Asimismo, el uso repetido de estas contraseñas aumenta las posibilidades de que las contraseñas sean deducidas, debido a que están en uso por períodos de tiempo considerablemente más prolongados que las otras contraseñas. La versión menos estricta de esta política omitiría las palabras “sustancialmente parecidas”.

Políticas Relacionadas: “[Contraseñas Cíclicas](#)” e “[Histórico de Contraseñas](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

6. Caracteres de las Contraseñas

Política: Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabetico y otro no alfabetico.

Comentario: Esta política informa a los usuarios que deben tomar medidas específicas para dificultar la deducción de las contraseñas por parte de personas no autorizadas y del software de penetración automatizada de sistemas. Existe una cantidad de pasos específicos que se pudiera ordenar a los usuarios. Estos pasos incluyen el uso de mayúsculas y minúsculas dentro de la misma contraseña. Cerciórese de verificar la documentación de los sistemas antes de redactar esta política, porque algunos sistemas tienen fuertes restricciones sobre el tipo de caracteres permitidos. Por lo general, los números de identificación personal (PIN, por sus siglas en inglés), que son un tipo de contraseña, se generan mediante un sistema de seguridad, por lo que no se aplica esta política. Estos PIN pueden utilizarse, por ejemplo, para activar tarjetas inteligentes o tarjetas portátiles con contraseña dinámica. Sin embargo, si estos PIN son seleccionados por el usuario, la cantidad de caracteres posibles podría quedar severamente restringida. No es posible combinar los caracteres alfabeticos con los caracteres no alfabeticos. Se deben tomar en consideración todos los sistemas posibles que utilizan las contraseñas seleccionadas por el usuario y los teclados disponibles, para que se esfuerzen por hacer que la política se aplique de manera consistente, tanto como sea posible.

Políticas Relacionadas:“[Estructura de las Contraseñas](#)” y “[Mayúsculas y Minúsculas en Contraseñas](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

7. Mayúsculas y Minúsculas en Contraseñas

Política: Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabetico en minúscula y uno en mayúscula.

Comentario: Esta política informa a los usuarios que deben tomar medidas específicas para dificultar la deducción de las contraseñas por parte de personas no autorizadas y del software de penetración automatizada de sistemas. Existe una cantidad de pasos específicos

que se pudiera ordenar a los usuarios. Estos pasos incluyen el uso de caracteres alfabeticos y no alfabeticos dentro de la misma contraseña. Desde el punto de vista matemático, la idea fundamental del uso de los caracteres en mayúscula y en minúscula es extender las contraseñas reales utilizadas de manera uniforme sobre todos los valores totales posibles, y así dificultar y hacer más costosa la deducción de contraseñas. La empresa debe cerciorarse de revisar la documentación de los sistemas antes de adoptar esta política, debido a que ciertos sistemas tienen fuertes restricciones sobre el tipo de caracteres permitidos.

Políticas Relacionadas:“[Estructura de las Contraseñas](#)” y “[Caracteres de las Contraseñas](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

8. Histórico de Contraseñas

Política: Se deben utilizar un software del sistema y un software desarrollado a nivel local para mantener un histórico cifrado de contraseñas fijas anteriores, que contenga las 13 contraseñas anteriores de cada identificador de usuario.

Comentario: La seguridad suministrada por los cambios requeridos de contraseñas resulta mucho menos efectiva si los usuarios repiten las mismas contraseñas. El archivo histórico evita que los usuarios alternen entre dos contraseñas o sigan algún otro esquema de rotación con una pequeña cantidad de contraseñas. Algunos sistemas operativos suministran este mecanismo de seguridad. Es importante establecer una política multi-plataforma para la gestión de contraseñas, especialmente si la empresa utiliza en la actualidad sistemas de acceso único o tiene la intención de implementarlos. En esta política se proporciona una parte de la política multi-plataforma que sirve para administrar las contraseñas. Adicionalmente, ciertas empresas querrán especificar que el proceso de cifrar una contraseña debe ser por una sola vía, de modo que no se puedan descifrar las contraseñas guardadas. Aunque ya no se utilizan las contraseñas históricas, lo deseable es mantenerlas fuera de la disponibilidad absoluta de personas no autorizadas, de modo que no puedan aplicar sus conocimientos para predecir contraseñas en el futuro. Ciertas organizaciones querrán incrementar por encima de 13 la cantidad mínima de contraseñas guardadas en el archivo histórico.

Políticas Relacionadas:“[Cambios Obligatorios de Contraseña](#)” y “[Contraseñas Cíclicas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

9. Semilla para Contraseñas Generadas por el Sistema

Política: Si se utilizan contraseñas generadas por el sistema, éstas deben generarse utilizando bits del reloj del sistema de orden inferior u otras fuentes no predecibles que puedan cambiar con frecuencia.

Comentario: Debido a que las contraseñas son con frecuencia la única defensa que protege el sistema, éstas deben crearse con mucho cuidado si se pretende soportar diversos tipos de ataque. Las contraseñas generadas por el sistema pueden cambiar de inmediato si el atacante logra obtener acceso al algoritmo utilizado en la generación de contraseñas y si éste tiene acceso a una fuente predecible de entradas a este algoritmo. Dado que es dudosa la reserva progresiva de un algoritmo que genere contraseñas, especialmente cuando forma parte de un sistema operativo o cualquier otro software diseminado ampliamente, es importante que las entradas al algoritmo sean impredecibles. Por ejemplo, ya se pueden obtener varios algoritmos de generación de contraseñas por el sistema en los foros de hackers o en el dominio público. El punto de partida de estos cálculos debe resultar muy difícil de predecir para las personas no autorizadas. Sin embargo, en el mundo real, bastará con los parámetros de semilla que cambian con frecuencia, o mejor aún, con una combinación de parámetros de semilla que cambian con frecuencia. También son importantes en esta política las palabras "que puedan cambiar con frecuencia". Si se utilizan fechas actuales u otra sucesión de caracteres predecibles que cambian con poca frecuencia para la generación de contraseñas, se podrían deducir con facilidad las contraseñas resultantes. Esta misma política puede utilizarse para los procesos de generación de claves de cifrado.

Políticas Relacionadas:["Generación de Claves de Cifrado"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

10. Contraseñas Generadas por el Sistema

Política: Todas las contraseñas generadas por el sistema destinadas a los usuarios finales deben ser pronunciables.

Comentario: Las contraseñas generadas por el sistema al estilo de "IDTP2EA9" ruegan ser escritas en alguna parte, porque son difíciles de recordar. Por otra parte, las contraseñas generadas por el sistema como "cabelloverdecome" se pueden recordar con mayor facilidad y existen menos probabilidades de escribirlas. Esta política ayuda a crear estas contraseñas con componentes pronunciables, que son casi siempre sílabas. Si bien no es necesario crear contraseñas generadas por el sistema haciendo una sucesión de palabras sacadas del diccionario, ayuda el hecho de construirlas con palabras pronunciables. Si bien el enfoque descrito en esta política hace que las contraseñas generadas por el sistema sean recordadas con mayor facilidad, también restringe severamente el dominio de contraseñas posibles totales, y por lo tanto, reduce la seguridad que proporcionan las contraseñas generadas por el sistema. Una forma de compensar esto es aumentar la cantidad mínima de caracteres en las contraseñas generadas por el sistema, tal vez a 15 caracteres. Otra propuesta es permitir a los usuarios hacer su selección a partir de un listado de 10 o más contraseñas posibles generadas por el sistema. Este listado de contraseñas posibles se generaría de una manera distinta para cada usuario final. Algunos de estas contraseñas generadas por el sistema son utilizadas para administrar claves de cifrado de manera transparente para el usuario final, firmas digitales, códigos de autentificación de mensajes y otros procesos relacionados con la seguridad.

Políticas Relacionadas:["Generación de Claves de Cifrado"](#)

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

11. Emisión y Almacenamiento de Contraseñas Generadas por el Sistema

Política: Si las contraseñas o los números de identificación personal son generados mediante un sistema de computación, éstos deben siempre emitirse inmediatamente después de que sean generados y nunca se deben almacenar en los sistemas de computación involucrados.

Comentario: Esta política garantiza que las contraseñas generadas y no emitidas no caerán en manos equivocadas. No se recomienda guardar las contraseñas generadas por el sistema en un computador, incluso en forma cifrada. La única oportunidad en la que se deben guardar las contraseñas en un sistema es cuando estén cifradas con una función de una sola vía, lo cual evita que sean descifradas, incluso por personas autorizadas.

Si se guardan estas contraseñas, utilizando la función de una sola vía, éstas no pueden reconstruirse en forma legible y, en caso de que ocurra, éstas no pueden emitirse nuevamente. Las contraseñas deben emitirse en el momento en que éstas se generen. Asimismo, esta política podría utilizarse como justificación para restringir las indagaciones que comprueben la operación de una rutina de generación de contraseñas, así como las llamadas que hagan programas no autorizados a las rutinas de contraseñas generadas por el sistema. Esta política permite generar las contraseñas y números de identificación personal a solicitud del usuario en forma de tiempo real o en lotes. En caso de que se haga a solicitud del usuario, lo normal es que el usuario se presente con varias contraseñas y se le pide seleccionar una de ellas. Posteriormente, se guarda la contraseña seleccionada en un archivo destinado para tal fin, utilizando la función de una sola vía. Si se hace en forma de lotes, las contraseñas se utilizarían para programar tarjetas inteligentes, codificar las barras magnéticas de las tarjetas plásticas de los cajeros automáticos, imprimir envases seguros para envío de correos, o realizar otras actividades relacionadas con la seguridad. Igualmente, se puede utilizar la misma política para la construcción de claves de cifrado.

Políticas Relacionadas: “[Recuperación de Contraseñas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

12. Materiales para la Generación de Contraseñas

Política: Todos los medios de almacenamiento computarizado o áreas de la memoria de un computador que sean utilizados en la creación, asignación, distribución o cifrado de contraseñas o de números de identificación personal, deben reescribirse reiteradamente con una serie de unos y ceros, inmediatamente después de utilizados.

Comentario: Es necesario reescribir una serie de unos y de ceros, porque los medios magnéticos de los computadores pueden suministrar una señal débil que refleje los valores anteriores de los datos, en lugar de su valor real. Resultará insuficiente la reescritura de los datos en una sola oportunidad en ambientes de alta seguridad. Sin este proceso de escritura múltiple, personas conocedoras de medios magnéticos podrían reconstruir los datos de varias generaciones atrás. Esta técnica evita que los programas de uso práctico y las aplicaciones no autorizadas tengan acceso a las áreas de memoria que

contienen las contraseñas, los números de identificación personal o los datos utilizados para crear estos parámetros de seguridad. En ciertos ambientes de muy alta seguridad, tal como ocurre en las unidades militares, se deben destruir los medios magnéticos que contengan información sensible, quemándolos, rompiéndolos en pedazos o mediante cualquier mecanismo relacionado, debido a que su reescritura no proporciona suficiente seguridad. En estos casos, no basta con la seguridad que proporciona la propuesta descrita en esta política. Esta misma política podría utilizarse para la creación de claves de cifrado.

Políticas Relacionadas: “[Algoritmos Generadores de Contraseñas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

13. Algoritmos Generadores de Contraseñas

Política: Se deben controlar el software y todos los archivos que contengan fórmulas, algoritmos y otros puntos específicos del proceso utilizado para generar las contraseñas o números de identificación personal, con las medidas de seguridad más estrictas que soporte el sistema de computación correspondiente.

Comentario: Esta política es información sobre el proceso mediante el cual se crean las contraseñas generadas por el sistema y debe recibir la protección más estricta. Si se divultan los puntos específicos sobre el proceso crítico de seguridad a personas no autorizadas, todo el sistema quedaría comprometido. Por esta razón, el mecanismo de generación de contraseñas forma parte del núcleo, la parte más protegida de ciertos sistemas operativos. Ciertas organizaciones desearían incluir documentación, papeleo ocasional y otros materiales utilizados para generar contraseñas dentro del ámbito de esta política.

Políticas Relacionadas: “[Materiales para la Generación de Contraseñas](#),” “[Cifrado de Contraseñas](#),” y “[Sistemas de Gestión de Claves de Cifrado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

14. Visualización e Impresión de Contraseñas

Política: Se debe disfrazar, suprimir, o de algún modo ocultar la visualización e impresión de las contraseñas, de manera tal que las personas no autorizadas no puedan observarlas o recuperarlas posteriormente.

Comentario: Esta política evita que las contraseñas caigan en manos de personas no autorizadas. En el momento en que el usuario escribe una contraseña en el sistema, el monitor no debe mostrar la contraseña o imprimirse en un terminal de papel. Si se mostrara la contraseña, las personas cercanas podrían mirar por encima del usuario para obtener la contraseña. Las personas que pasen por el archivo de papelera podrían recuperar las contraseñas impresas en el terminal de copias en papel. Para la pantalla, el mecanismo que se utiliza con cierta frecuencia es un eco apagado al momento de introducir la contraseña. Para los terminales de copias en papel se utiliza a veces la repetición de teclas encima de ellas mismas, múltiples veces. En ocasiones es posible recuperar las contraseñas de archivos temporales o de ubicaciones casuales en la memoria.

Políticas Relacionadas: “[Materiales para la Generación de Contraseñas](#),” “[Posiciones de las Pantallas de los Computadores](#),” y “[Contraseñas Iniciales](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

15. Máscaras para Cambios de Contraseña

Política: Cada vez que se especifiquen las contraseñas seleccionadas por los usuarios o las claves de cifrado, éstas deben introducirse dos veces y enmascararse.

Comentario: Esta política evita que se produzcan problemas al cometer errores involuntarios de digitación. Debido a que el enmascaramiento evita que los usuarios vean los caracteres que ingresan, si no se introducen dos veces, los usuarios no tienen idea de que han cometido un error de digitación. La confirmación de una contraseña o clave de cifrado, también conocida como la doble entrada de estos parámetros, a menudo, aunque no siempre, revela este problema. Existen otros mecanismos de control para aquellas situaciones poco comunes en las que este enfoque no detecta un error de digitación porque el mismo error se comete dos veces. Esta política hace referencia a los casos en que un usuario especifica una contraseña, por ejemplo cuando cambia la contraseña. De la misma manera, esta política trata con las claves de cifrado que pueden ingresarse cuando un archivo está a punto de ser cifrado. La política no necesita aplicarse a los casos en que el usuario intenta acceder a un sistema utilizando una contraseña previamente especificada, porque el sistema le informará al usuario que ha introducido una contraseña equivocada y lo invitará a intentarlo nuevamente. Asimismo, si se provee una clave de

cifrado incorrecta en el momento de descifrar un archivo, el programa dará resultados ininteligibles o una notificación de error.

Políticas Relacionadas: “[Almacenamiento de Contraseñas Legibles](#)” y “[Ocultar Números de Cuenta de Clientes](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

16. Cambios Obligatorios de Contraseña

Política: Todos los usuarios deben ser obligados automáticamente a cambiar sus contraseñas al menos una vez cada 90 días.

Comentario: Esta política obliga a los usuarios a cambiar sus contraseñas con cierta periodicidad. No hay nada particular acerca del período de 90 días mencionado en la política. Podría fácilmente ser otro lapso de tiempo. Si la necesidad de seguridad es grande, el intervalo podría ser más corto. De hecho, algunas organizaciones tienen un enfoque de niveles mediante el cual se emplean diferentes intervalos de tiempo de acuerdo con las distintas poblaciones usuarias, en función de la naturaleza de los privilegios disponibles para estos usuarios. Por ejemplo, a los programadores de sistemas se les debe solicitar que cambien su contraseña cada dos semanas, mientras que a los usuarios comunes se les puede pedir que lo hagan una vez al mes. Sin el proceso de solicitud de cambio de contraseña, si una contraseña ha caído en manos de un tercero no autorizado, el uso no autorizado del sistema podría continuar por algún período de tiempo. Esta política limita este lapso de tiempo. Asimismo, si se combina con el proceso de revocación de privilegios de un identificador de usuario inactivo, esta política actúa como una red de seguridad en caso de que los administradores del sistema olviden inhabilitar los privilegios cuando los usuarios cambian sus funciones o abandonan una organización. Esta política limita el lapso de tiempo en el cual este compañero de trabajo puede hacerse pasar por otro usuario al compartir su contraseña. Dos efectos secundarios indeseables asociados con los cambios frecuentes de contraseñas son aquellos en que los usuarios escriben sus contraseñas o desarrollan algoritmos fáciles para generar contraseñas que pueden ser adivinadas por terceros no autorizados. A menos que esté involucrado un ambiente de alta seguridad, la organización debe abstenerse de establecer la frecuencia de cambio en un lapso de tiempo inferior a los 60 días. Esta política funciona bien cuando se combina con una

política que exija que las contraseñas sean cambiadas cuando se comprometa o se sospeche que se ha comprometido el sistema de seguridad de contraseñas.

Políticas Relacionadas: "Sospecha de Divulgación de Contraseña," "Estructura de las Contraseñas," "Sincronización de los Intervalos de Cambios de Contraseñas," y "Cambio de Números Discados"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Sincronización de los Intervalos de Cambios de Contraseñas

Política: El intervalo de cambio de las contraseñas fijas debe estar sincronizado a lo largo y ancho de todas las plataformas de computación y redes de la Empresa X.

Comentario: Esta política establece la infraestructura para los sistemas de acceso único, en los que los usuarios pueden conectarse una sola vez, pero dentro de una misma sesión en línea pueden utilizar múltiples sistemas. Esta política también es útil en términos de preparación para el uso de los servidores de seguridad, a través de los cuales puede ocurrir la administración de plataformas múltiples. Esta política también es amigable para los usuarios debido a que les permite simplificar sus actividades de administración de contraseñas, utilizando una única contraseña fija para múltiples sistemas. Algunos expertos en seguridad se quejan de que éste es un enfoque riesgoso, pero en el mundo real los usuarios se encuentran sobrecargados con la complejidad de los sistemas de seguridad informática, y dan la bienvenida a cualquier movimiento en dirección a la simplificación. Si las contraseñas fijas son utilizadas en un ambiente de alta seguridad y son transmitidas sin haber sido cifradas, entonces este enfoque es riesgoso. Pero si existe un ambiente de baja seguridad o las contraseñas fijas son cifradas cuando son enviadas y almacenadas, entonces la sincronización de contraseñas mencionada en esta política tiene sentido y es recomendable. Esta política asume que los usuarios son capaces de cambiar sus contraseñas siempre que lo deseen. La existencia de esta capacidad les permitirá cambiar todas sus contraseñas en todos los sistemas en una fecha determinada.

Políticas Relacionadas: "Cambios Obligatorios de Contraseña" y "Cambios de Seguridad Despues de Estar Comprometido el Sistema"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

18. Contraseñas Legibles

Política: Las contraseñas fijas nunca deben encontrarse en forma legible fuera del computador personal o de la estación de trabajo.

Comentario: Esta política brinda una guía para la construcción, integración y administración de los sistemas de control de acceso basados en contraseñas. A pesar de que las contraseñas dinámicas son más deseables, muchas organizaciones están utilizando las contraseñas fijas. Esta política permite que las contraseñas fijas las continúe empleando el usuario final. Debido a que las contraseñas fijas en forma legible pueden ser fácilmente capturadas cuando viajan por una red, es crítico que sean cifradas cuando se encuentren en una red o en otros lugares rápidamente accesibles. No es suficiente el cifrado simple. El cifrado debe ser implementado de forma tal que las contraseñas aparezcan en forma diferente cada vez que viajan por la red y sean utilizadas. Si esto no ocurre, los atacantes pueden utilizar métodos de reproducción para causar fraude, sabotaje y otros abusos. Esta política es consistente con los productos comerciales que permiten que las contraseñas sean almacenadas en claves de acceso. En general, esta clase de almacenamiento de contraseñas es una práctica peligrosa debido a que personas no autorizadas pueden utilizar estas contraseñas. Esta política es particularmente apropiada para los sistemas cliente-servidor, redes de área local y otros sistemas pequeños.

Políticas Relacionadas: "Almacenamiento de Contraseñas Legibles" y "Acceso a la Red"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

19. Información de Control de Acceso en Cookies

Política: Los sistemas informáticos de la Empresa X nunca deben almacenar ninguna información de control de acceso en "cookies" depositados o almacenados en computadores de los usuarios finales.

Comentario: Esta política evita el acceso no autorizado a los sistemas informáticos de la Empresa X. Los "cookies" son pequeños archivos que están depositados en computadores remotos conectados a través de Internet. Los "cookies" pueden ser almacenados permanentemente en un disco duro o pueden ser borrados cuando se ha completado la sesión de Internet o cuando el usuario sale del explorador. Esta política ha sido redactada de forma que se refiera a ambas clases de

archivos "cookie". A pesar de que este enfoque es popular para algunos comerciantes web, tiene serios inconvenientes. Es popular porque los usuarios no necesitan recordar un identificador de usuario o una contraseña fija y por lo tanto pueden conectarse automáticamente. Sin embargo, si una persona no autorizada se sentara en el computador de un usuario autorizado y pudiera dirigir el buscador a uno de estos mismos comerciantes web, entonces la persona no autorizada se conectaría automáticamente. A pesar de que ésta podría parecer una posibilidad remota, no lo es si el usuario no autorizado visita aquellos sitios marcados como favoritos en el explorador por el usuario autorizado. Esta conexión no intencional podría permitirle a la persona no autorizada comprar productos en nombre del usuario autorizado, descubrir su información privada o personificarlo en el correo electrónico u otras comunicaciones. Esta política ha sido deliberadamente redactada en forma general de manera que prohíba a los desarrolladores almacenar privilegios de control de acceso en "cookies".

Políticas Relacionadas:“[Cookies para Inicios Automáticos de Sesión](#)” y “[Cookies](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

20. Cifrado de Contraseñas

Política: Las contraseñas siempre deben cifrarse cuando se almacenen por un lapso significativo de tiempo o cuando se transmitan a través de las redes.

Comentario:El cifrado provee una de las pocas maneras efectivas de salvaguardar las contraseñas fijas, las claves de cifrado, los generadores de números seudo-aleatorios y otros parámetros de seguridad. Sin el cifrado, estos parámetros pueden ser divulgados inadvertidamente a personas que tienen acceso a la memoria intermedia de sistemas de telecomunicación o a la memoria temporal del computador. Programas especiales tipo rapiña también pueden utilizarse para registrar parámetros de seguridad descifrados para su subsiguiente recuperación por parte de personas no autorizadas. Esta política garantiza que los diseñadores de sistemas siempre utilizarán el cifrado para proteger los parámetros de seguridad como las contraseñas. Idealmente, la clase de cifrado asegurará que la cantidad cifrada varíe en el tiempo, a pesar de que no ocurra lo mismo con la cantidad descifrada. El término "se almacenen por un lapso significativo de tiempo", se utiliza para excluir las ubicaciones internas de memoria dentro de un sistema que pudiera contener una

contraseña descifrada. Esta política es particularmente relevante para las comunicaciones en Internet, y puede ser redactada de manera que se restrinja a dichas comunicaciones. Muchos programas de recopilación de contraseñas han sido utilizados para comprometer la seguridad en Internet.

Políticas Relacionadas:“[Materiales para la Generación de Contraseñas](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

21. Recuperación de Contraseñas

Política: Los sistemas de computación y comunicación deben ser diseñados, probados y controlados para prevenir tanto la recuperación como el uso no autorizado de las contraseñas almacenadas, se encuentren éstas en forma cifrada o descifrada.

Comentario:Esta política evita que personas no autorizadas obtengan acceso a contraseñas que podrían ser utilizadas para lograr acceso no autorizado al sistema. Cuando un usuario introduce una contraseña, ésta debe ser cifrada utilizando una función de una vía, y esta nueva cadena cifrada debe entonces ser comparada con la cadena cifrada pertinente en el archivo de contraseñas de la máquina del destinatario. Las cadenas cifradas que se encuentran en el archivo de contraseñas nunca deberían ser recuperables por los usuarios debido a que esto permitiría que se montara un ataque tipo diccionario. Un ataque diccionario involucra el cifrado de las entradas de un diccionario legible por computador y la comparación posterior de estas cantidades con las entradas en el archivo de contraseñas. Si se produce una coincidencia, se ha descubierto una versión descifrada de la contraseña. Esta contraseña puede utilizarse para comprometer la seguridad del sistema involucrado. Inclusive cuando se utilizan las funciones de cifrado de una vía, puede montarse el ataque diccionario. Para evitar esta clase de ataques, esta política emplea controles de acceso de forma tal que se eviten todas las recuperaciones de contraseñas. El mismo concepto puede extenderse a las claves de cifrado, generadores de números seudo-aleatorios y otros parámetros de seguridad. Existen otros controles que cumplen los objetivos especificados en esta política, pero estos controles adicionales deben ser identificados e implementados por la gerencia local con base en los requerimientos del sistema informático.

Políticas Relacionadas:“[Emisión y Almacenamiento de Contraseñas Generadas por el Sistema](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

22. Contraseñas de Control de Acceso al Sistema

Política: El control de acceso a computadores y sistemas de comunicación debe llevarse a cabo a través de contraseñas únicas para cada usuario individual.

Comentario: Esta política evita que los administradores de sistemas establezcan privilegios de control de acceso con un esquema que pueda conducir a problemas, por ejemplo utilizando contraseñas especiales (lockwords) que se utilizan para manejar el control de acceso a un archivo, pero que pueden pasarse con facilidad a otro usuario. El Propietario del archivo que originalmente otorgó el acceso puede rápidamente perder el control sobre quién tiene acceso y quién está cambiando el archivo. Esto derrota el principio de responsabilidad individual con el que se intenta atribuir a cada individuo el evento de sistema que le corresponda. El uso de un identificador de usuario individualizado y una contraseña propia, conjuntamente con los privilegios de acceso correspondientes, previene la disseminación secundaria de las contraseñas porque las contraseñas deben permanecer de exclusivo conocimiento del usuario correspondiente. Esta política es consistente con el uso de dispositivos de identidad portátiles o con sistemas de autenticación extendida de usuarios. Nada de lo mencionado en esta política sugiere que estos sistemas no puedan usarse además de los sistemas de contraseñas fijas. La política también prohíbe el compartir identificadores de usuario con cuentas grupales. Esta política es relevante para sistemas telefónicos, redes de área local, sistemas cliente-servidor y otros sistemas de comunicaciones, aparte de los paquetes tradicionales de control de acceso estilo mainframe.

Políticas Relacionadas:“[Contraseñas Compartidas](#)”, “[Identificador Unico de Usuario y Contraseña Obligatorios](#),” e “[Identificadores de Usuarios Unicos](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

23. Contraseñas Proporcionadas por Proveedores

Política: Todas las contraseñas predeterminadas suplidas por el proveedor deben ser cambiadas antes de que algún computador o sistema de comunicaciones sea utilizado para el negocio de la Empresa X.

Comentario: Una de las más antiguas pero más exitosas maneras de ingresar a los sistemas es la de emplear las contraseñas predeterminadas por los proveedores. Por lo general, éstas son conocidas tanto por el personal técnico con experiencia en esta plataforma como por la comunidad de hackers. Algunas organizaciones olvidan cambiar estas contraseñas antes de colocar sus sistemas en modo producción. Esta política notifica al personal técnico que debe cambiar todas las contraseñas predeterminadas del proveedor para alcanzar el más básico nivel de seguridad. Para restringir el alcance de esta política, la palabra "producción" puede añadirse a la misma, tal vez acompañada de una definición si la audiencia no está familiarizada con la noción de sistemas de producción. Esta política es particularmente importante en los ambientes de computación conectados a Internet, sistemas cliente-servidor, redes de área local y sistemas pequeños en donde los administradores de sistemas pueden no estar ampliamente adiestrados en el procesamiento de datos. Algunos paquetes de identificación de vulnerabilidades pueden ser utilizados para monitorear la conformidad con esta política.

Políticas Relacionadas:“[Contraseñas Iniciales](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

24. Cambios de Seguridad Despues de Estar Comprometido el Sistema

Política: Cada vez que un sistema esté comprometido o se sospeche que se ha comprometido por un tercero no autorizado, los gerentes del sistema deben recargar inmediatamente una versión confiable del sistema operativo y de todo el software relacionado con la seguridad, y todos los cambios recientes de privilegios de usuarios y del sistema deben ser revisados para verificar los cambios no autorizados.

Comentario: El propósito de esta política es restablecer un sistema operativo seguro y todos los controles de acceso basados en contraseñas después de una irrupción o de que las medidas de seguridad se vean comprometidas. Se requiere una respuesta inmediata porque mientras más tiempo pasen dentro del sistema las partes no autorizadas, más oportunidad tendrán de establecer

identificadores de usuarios no autorizados, privilegios no autorizados para los identificadores de usuarios existentes sobre los cuales tengan control, y escotillas que les permitan acceso futuro al sistema. Al recargar el sistema operativo y explorar los accesos para determinar si existen cambios no autorizados y deshacerlos, se ayudará a eliminar una posterior actividad no autorizada. Además de ser relevante para los operadores del departamento de Sistemas Informáticos, esta política se aplica a los administradores de servidores de redes de área local, gerentes departamentales de sistemas de computación y personas similares que se encuentren

9.05.05 Uso de las Utilidades del Sistema

1. Selección de Herramientas de Seguridad

Política: Antes de distribuir software para identificación de vulnerabilidad u otras herramientas que puedan ser utilizadas para comprometer la seguridad de los sistemas informáticos, el personal de la Empresa X debe investigar y validar la necesidad del receptor de estas herramientas.

Comentario: Esta política pretende restringir la distribución de herramientas que puedan ser utilizadas para comprometer la seguridad de los sistemas informáticos. Esta política puede ser ampliada e incluir información de seguridad sensible que pueda ser utilizada para comprometer la seguridad de los sistemas. Aunque está dirigido principalmente para ser empleado por desarrolladores de software y otras organizaciones que producen o distribuyen estas herramientas, el concepto descrito en la política es aplicable generalmente a todas las organizaciones. Esta política pretende evitar que la organización distribuidora se considere responsable de cualquier daño causado con su herramienta. Un texto que acompañe a esta política puede especificar cómo debe validar el personal la necesidad del receptor de esta herramienta

Políticas Relacionadas: “Prueba de los Controles del Sistema Informático,” “Herramientas de Estado de Seguridad del Sistema,” “Poderosas Herramientas de Sistemas Informáticos,” y “Evidencia de Delito o Abuso Informático”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

ubicadas dentro de la organización en posiciones fuera del departamento de Sistemas Informáticos. Esta política es particularmente importante para aquéllos a cargo de pequeños sistemas como los sistemas cliente-servidor y las redes de área local.

Políticas Relacionadas: “Sospecha de Divulgación de Contraseña”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Software de Identificación de Vulnerabilidades

Política: Cuando el software de identificación de vulnerabilidades no se está utilizando activamente, debe ser removido del sistema en el que se estaba ejecutando.

Comentario: El propósito de esta política es asegurar que partes no autorizadas no utilicen el software de identificación de vulnerabilidades para irrumpir dentro de los sistemas de la Empresa X. Si no se remueve este software, es posible que un intruso pueda utilizarlo en su provecho. Aunque el uso de software para identificación de vulnerabilidades se encuentra ampliamente distribuido, los especialistas técnicos a veces no comprenden cuán peligrosas son estas herramientas si caen en las manos equivocadas. Asimismo, no entienden cómo este software puede ser utilizado para atacar a los sistemas administrados por otras organizaciones y cómo sus empleados pueden ser responsables por estas intrusiones. Esta política se aplica a aquellas situaciones en las que el software se ejecuta en un sistema centralizado que prueba sistemas remotos, y situaciones en las que el software se ejecuta en sistemas distribuidos que reportan a un sistema centralizado.

Políticas Relacionadas: “Identificación de Vulnerabilidades” y “Evidencia de Delito o Abuso Informático”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Poderosas Herramientas de Sistemas Informáticos

Política: Todas las herramientas poderosas de los sistemas informáticos construidas o distribuidas por la Empresa X que puedan ser empleadas para provocar un

daño significativo deben ser automáticamente restringidas de forma que únicamente puedan ser utilizadas para cumplir su propósito original.

Comentario: Esta política tiene como objetivo guiar a los desarrolladores en la selección de una funcionalidad apropiada. Los mecanismos específicos a utilizar no están deliberadamente especificados en la política a menos que esto restrinja excesivamente a los desarrolladores. La política instruye al personal a ayudar a limitar la obligación del desarrollador o del distribuidor. Esta política se aplica a una amplia variedad de productos como los discos flexibles, no únicamente a las herramientas de seguridad informática.

Políticas Relacionadas: “[Prueba de los Controles del Sistema Informático](#),” “[Herramientas de Estado de Seguridad del Sistema](#),” “[Poderosas Herramientas de Sistemas Informáticos](#),” y “[Evidencia de Delito o Abuso Informático](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Herramientas de Estado de Seguridad del Sistema

Política: Todo sistema multiusuario debe poseer las suficientes herramientas automatizadas para asistir al administrador de seguridad en la verificación del estado de seguridad del computador y debe poseer mecanismos para la corrección de problemas de seguridad.

Comentario: Esta política debe ser utilizada en el proceso de adquisición de sistemas de computación nuevos o mejorados. También puede ser útil en la adquisición de herramientas para asistir a los administradores en el mantenimiento de un nivel adecuado de seguridad de los sistemas. Esta política requiere que todo sistema multiusuario posea suficientes herramientas para determinar si la seguridad es adecuada y si los mecanismos de seguridad están funcionando como deberían. Estas herramientas podrían incluir paquetes de software que verifiquen la consistencia lógica de los privilegios asignados a los usuarios, la revisión automática de las conexiones al sistema o la verificación automática de que los parámetros de seguridad establecidos coinciden con la política de la organización. Los computadores personales no fueron incluidos en forma deliberada dentro del ámbito de esta política porque estas herramientas son poco comunes en esa clase de sistemas.

Políticas Relacionadas: “[Evidencia de Delito o Abuso Informático](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Hardware y Software de Diagnóstico

Política: El acceso a hardware y software para pruebas de diagnóstico debe ser estrictamente controlado y debe utilizarse únicamente por personal autorizado con propósitos de prueba, resolución de problemas y desarrollo.

Comentario: El hardware y software para pruebas de diagnóstico puede ser utilizado para insertar mensajes no autorizados dentro de una línea de comunicaciones de forma tal que pueda perpetrarse un fraude. Las herramientas también pueden permitir que las personas puedan leer la línea de tráfico de comunicaciones que de otra manera no podrían examinar. Estas herramientas para interceptar comunicaciones, han sido utilizadas, por ejemplo, para capturar contraseñas legibles e identificadores de usuarios que se emplearían posteriormente para obtener acceso no autorizado. Esta política restringe el uso de estas poderosas herramientas en la resolución de problemas y otras actividades de negocio autorizadas. Esta política le da una significativa flexibilidad a la gerencia local para determinar las maneras en las que podrán asegurar estas herramientas de hardware y software. Por ejemplo, algunos gerentes requerirán que los dispositivos de monitoreo de líneas se encuentren bajo llave en un closet, mientras que otros estarán satisfechos con el uso de una llave metálica para activar o desactivar el dispositivo. Existe una gran necesidad de esta política en aquellos ambientes que utilizan contraseñas fijas para el control de acceso a los sistemas. Esto se debe a que el monitoreo de líneas de comunicación puede ser utilizado para interceptar las contraseñas fijas. Asimismo, esta política no es necesaria, o al menos mucho menos necesaria, en aquellos ambientes en los que todo el tráfico de la red es cifrado.

Políticas Relacionadas: “[Mal Funcionamiento del Control de Acceso](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Almacenamiento de Utilidades del Sistema

Política: Los discos y demás facilidades de almacenamiento en línea utilizados en los sistemas de producción no deben contener compiladores, ensambladores, editores de texto, procesadores de palabras u

otros programas utilitarios de propósito general que puedan ser empleados para comprometer la seguridad del sistema.

Comentario: A pesar de la fuerte postura que se toma en esta política, de vez en cuando se podrá requerir el uso de estos programas utilitarios en casos de emergencia. En forma práctica, para cumplir con estas necesidades excepcionales, los programas utilitarios se pueden mantener en una cinta o disco bajo llave en un archivador en el cuarto de computación. Después de ser utilizadas, pueden ser borradas del sistema y la cinta o disco puede ser colocado nuevamente bajo llave en el archivador. Esta política es igualmente importante para sistemas más pequeños, como los sistemas cliente-servidor, servidores de redes de área local y sistemas de computadores personales, a pesar de que es más difícil de controlar. En estos ambientes, el software para administración de licencias de software se puede utilizar para identificar dichos programas utilitarios. Esta política evita que puedan ser fácilmente accesibles a los usuarios, reduciéndose las posibilidades de que sean empleados para evadir los controles. Algunos de los programas utilitarios mencionados en la política pueden necesitarse en determinados ambientes, por lo que pueden borrarse de la lista de programas utilitarios que se encuentran en esta política.

Políticas Relacionadas: “Uso de las Utilidades del Software del Sistema” y “Remoción de Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

7. Uso de las Utilidades del Software del Sistema

Política: El acceso a los programas utilitarios del sistema debe estar restringido a un número pequeño de usuarios confiables y autorizados y cada vez que dichos programas sean ejecutados, la actividad resultante debe ser registrada en forma segura y revisada por el gerente de Operaciones de Computación.

Comentario: La mayoría de los sistemas multiusuario poseen uno o más programas utilitarios que pueden ser utilizados para pasar por encima de los sistemas de control de acceso o de los controles de acceso de las aplicaciones. Como ejemplo se tienen las herramientas para solucionar problemas en una base de datos y los programas utilitarios para reparación del disco. Estas herramientas pueden permitir que el usuario altere directamente la base de datos de nómina, el archivo para impresión de cheques de cuentas por pagar y otro grupo

de información residente en el computador sin pasar por los canales normales y los controles asociados. Esta política evita que los programas utilitarios peligrosos sean utilizados por personas no autorizadas. En aquellas circunstancias en las que dichos programas deban ser utilizados para efectuar un trabajo, esta política asegura que su uso sea consistente con las intenciones de la gerencia. Con las palabras "registrada en forma segura" esta política también requiere de facilidades que identifiquen rápidamente el uso de programas utilitarios no autorizados. Esta política asume que los sistemas poseen controles de acceso como los basados en contraseñas y privilegios de los usuarios. Si muchas personas tienen acceso a los programas utilitarios en un sistema multiusuario, entonces los controles de acceso no son efectivos. La frase "registrada en forma segura" significa que debe registrarse de forma que no sea fácilmente modificable por los usuarios empleando el programa utilitario adecuado. A pesar de que pocas veces se hace, algunas organizaciones pueden querer ir más allá de lo expresado en esta política. Pueden querer autorizar específicamente cada vez que se utilice un programa utilitario del sistema.

Políticas Relacionadas: “Almacenamiento de Utilidades del Sistema,” “Cambios del Sistema Operativo de Producción,” y “Registro de Eventos Importantes de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Facilidades para Inhabilitar Controles

Política: La gerencia debe establecer y restringir el uso de las facilidades de inhabilitación que deban utilizarse en circunstancias excepcionales en las que los controles deben ser comprometidos para poder mantener las operaciones actuales del negocio.

Comentario: Esta política informa a los diseñadores de sistemas, programadores de aplicaciones y demás personal técnico acerca de la necesidad de contar con facilidades de inhabilitación. Esta política también pretende describir las intenciones de la gerencia con relación al uso de estas facilidades e indicar cómo se deben definir los controles de acceso a estas facilidades. Algunas organizaciones también podrían desear añadir algunas palabras a la política requiriendo que todo uso de facilidades de inhabilitación sea registrado. Si estas facilidades son usadas regularmente, pueden inutilizar los controles. Es por esta razón que únicamente deben ser utilizadas en casos absolutamente necesarios.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#),” “[Uso de la Inhabilitación de los Controles](#),” y “[Registro de Inhabilitaciones](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Uso de la Inhabilitación de los Controles

Política: La gerencia debe definir claramente las circunstancias específicas y los procedimientos de autorización que deben seguirse cuando se deban inhabilitar los controles del sistema.

Comentario: Esta política especifica las circunstancias en las que pueden utilizarse las facilidades de inhabilitación de los controles del sistema. Haciendo referencia a estas instrucciones, el personal puede utilizar estas facilidades sin obtener la aprobación específica de la gerencia. Esto es útil, por ejemplo, si el sistema falla fuera del horario de oficina, el problema se ha presentado antes y la solución ya se conoce y se encuentra por escrito. En un caso como éste, no es necesario obtener la autorización específica de la gerencia para utilizar las facilidades de inhabilitación. Esta política también se puede aplicar a los sistemas pequeños como las redes de área local, sistemas cliente-servidor y estaciones de trabajo multiusuario. Algunas organizaciones también podrían desear añadir algunas palabras a la política, estableciendo que es necesario registrar todo uso de las facilidades de inhabilitación. Si estas facilidades son utilizadas regularmente, pueden inutilizar los controles.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#),” “[Facilidades para Inhabilitar Controles](#),” y “[Registro de Inhabilitaciones](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Control de Acceso para Restaurar Archivos

Política: Si los usuarios finales reciben la capacidad para restaurar sus propios archivos, no debe otorgárseles privilegios para restaurar los archivos de otros usuarios o para ver cuáles archivos de otros usuarios han sido respaldados.

Comentario: Esta política garantiza que los usuarios no emplearán un sistema de respaldo como una manera de evadir un sistema de control de acceso. Por ejemplo, en una red de área local, un usuario puede ser capaz de restaurar los archivos de desempeño del personal almacenados por su supervisor y de esta manera frustrar los controles de acceso aplicados normalmente a estos archivos. Únicamente el administrador de la red de área local o el administrador de seguridad pueden tener acceso a los archivos de respaldo de múltiples usuarios. Una manera de reforzar esta política es cifrar los archivos respaldados utilizando una o más claves únicas para cada usuario. Los administradores de redes de área local o de seguridad pueden verificar periódicamente los accesos para determinar cuáles usuarios restauraron cuáles archivos y si ocurrió una actividad abusiva. Algunos cortafuegos en Internet monitorean el volumen de tráfico saliente para determinar si ha habido un flujo excesivo de información. Otros cortafuegos disponibles comercialmente limitan el volumen de información saliente que puede ser enviada. Este mismo enfoque para reducir el volumen de datos puede ser utilizado para controlar la información de respaldo a la que tienen acceso directo los usuarios.

Políticas Relacionadas: “[Mal Funcionamiento del Control de Acceso](#),” “[Cifrado en Medios de Respaldo](#),” y “[Almacenamiento de Medios de Respaldo](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9.05.06 Alarmas Coercitivas para Salvaguardar a los Usuarios

1. Contraseñas de Presión

Política: Cada vez que se otorgue a un usuario el acceso a datos particularmente valiosos y sensibles, deben emplearse contraseñas coercitivas o de presión para señalar en forma encubierta al sistema que dicho usuario está siendo presionado para conectarse.

Comentario: Las contraseñas coercitivas pueden limitar los privilegios del usuario, activar registros de acceso adicionales, activar una alarma remota o iniciar

automáticamente otra clase de acción relacionada con la seguridad. Las contraseñas coercitivas son generalmente diferentes de las contraseñas regulares, aunque ambas le permitirán al usuario ingresar al sistema. Debido a que las contraseñas coercitivas se pueden emplear cuando la seguridad del usuario está en peligro, es recomendable continuar proporcionando algún acceso al sistema. La contraseña coercitiva es una forma conveniente para que el usuario alerte a los operadores del sistema que se encuentren de guardia o a otras personas de que algo

serio está sucediendo. En el caso de las actividades cotidianas de negocio, las contraseñas coercitivas no son necesarias.

Políticas Relacionadas: “[Interrupción del Sistema por Seguridad](#)” y “[Proyectos que Involucran Seguridad Humana](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Alto

9.05.07 Desconexión por Tiempo

1. Cierre de Sesión Automático

Política: Si no ha habido actividad en un terminal, estación de trabajo o computador personal por 10 minutos, el sistema debe automáticamente poner en blanco la pantalla, suspender la sesión y solicitar una contraseña para restablecer la sesión.

Comentario: Esta política evita la divulgación no autorizada de información y la utilización no autorizada del sistema en casos en que los empleados autorizados abandonan sus escritorios sin antes desconectarse. Particularmente, en aquellas oficinas abiertas en las que no hay paredes, muchas personas dejan sus computadores prendidos y disponibles para cualquiera que pase por allí. A pesar de que esta política es más efectiva cuando se aplica a todas las estaciones de trabajo, podría restringirse a los sistemas que contienen o acceden a información sensible, crítica o valiosa. En muchos casos, debido a que la desconexión automática no forma

parte del sistema operativo, para implementar esta política será necesario un paquete de software de seguridad para los computadores personales y estaciones de trabajo. Nada de lo mencionado en esta política requiere que un usuario pierda el trabajo que estaba desarrollando, porque después de introducir la contraseña adecuada, el trabajo puede continuar. El número de minutos puede ser ajustado en función del nivel de seguridad del sistema. Cuando no se dispone de software para desconexión automática, las organizaciones pueden adoptar una política en la que se exija que los usuarios se desconecten cuando abandonan sus estaciones de trabajo.

Políticas Relacionadas: “[Sesiones Activas Desatendidas](#)”

Activas

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9.05.08 Limitación del Tiempo de Conexión

1. Control de Acceso Crono-Dependiente

Política: Todos los sistemas de computación multiusuario deben emplear sistemas de identificación positiva de los usuarios para controlar el acceso tanto a la información como a los programas que se encuentran restringidos por la hora del día y el día de la semana.

Comentario: El control de acceso predeterminado que se encuentra en muchos sistemas se basa en varias clases de acceso a la información o a las aplicaciones. Las organizaciones que desean apoyar este ambiente de control, pueden promulgar restricciones adicionales en función a la hora y al día como se menciona en esta política. Esta política tiene como objetivo pedir mayores requerimientos aparte de los controles de acceso simples, normalmente basados en los identificadores de usuarios y las contraseñas. Esto no implica que se necesiten tarjetas inteligentes, biometría u otras tecnologías costosas. Además de los controles de acceso

dependientes del horario, otra forma fácilmente disponible y de bajo costo para ampliar los identificadores de usuarios y las contraseñas es a través de códigos de identificación en terminales o direcciones de red. Cada organización debe basar las medidas de control mediante identificación positiva del usuario en función a una valoración de riesgo. Estudios recientes acerca de la actividad de los hackers demuestran que son más activos en la noche, justo cuando los sistemas tienen escaso o ningún personal. Sin embargo, dado que actualmente muchas personas trabajan en horarios extravagantes, esta política puede restringirse a aquellas aplicaciones que manejan datos sensibles o valiosos, como los sistemas de transferencias cablegráficas. Esta política es muy relevante para las organizaciones que han establecido horarios oficiales de operación. La globalización que camina junto con el comercio en Internet y las redes internas de las organizaciones, pueden requerir que esta política sea redactada

nuevamente para reflejar los horarios locales. Esta política es pertinente en el caso de trabajos por lote y sesiones interactivas.

Políticas Relacionadas:“[Restricción de Privilegios — Necesidad de Conocer](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

9.06 Control de Acceso a las Aplicaciones

9.06.01 Restricción del Acceso a la Información

1. Contraseñas de Servicio al Cliente

Política: Las contraseñas fijas utilizadas para verificar la identidad de un cliente a través del teléfono nunca deben ser mostradas por los sistemas informáticos de la Empresa X.

Comentario:Esta política limita el número de empleados internos de la Empresa X que tienen acceso a las contraseñas de atención al cliente. Estas contraseñas por lo general son diferentes de las contraseñas de conexión. Si las contraseñas de atención al cliente fueran conocidas por los empleados internos, éstos podrían hacerse pasar por los clientes involucrados y comprometer a la empresa en fraude, invasión a la privacidad y otros abusos. Por ejemplo, el departamento de transferencias en muchos bancos utilizan contraseñas de atención al cliente que autorizan la divulgación de información confidencial del cliente para transferir fondos entre sus cuentas. Esta política describe un enfoque fácil de implementar en el que el sistema solamente provee una respuesta “correcta” o “incorrecta” a la contraseña digitada por el representante de atención al cliente. Este enfoque evita que los representantes de atención al cliente bien intencionados den pistas no autorizadas o decidan que la contraseña provista es lo suficientemente parecida a la que se encuentra almacenada en el sistema y por lo tanto procedan a efectuar transacciones sensibles o divulgaciones. Las pistas pueden ser soportadas oficialmente como parte del software en caso de que la gerencia lo decida. Esta política coincide con la noción de que únicamente el cliente o el usuario deben conocer sus contraseñas.

Políticas Relacionadas:“[Ocultar Números de Cuenta de Clientes](#)” y “[Comprometer Mecanismos de Seguridad para los Clientes](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

2. Identificadores de Usuario o Contraseñas Secretas

Política: Los desarrolladores no deben construir o desplegar identificadores de usuarios secretos o contraseñas que tengan privilegios especiales y que no se encuentren claramente descritos en la documentación generalmente disponible del sistema.

Comentario:Esta política está orientada a atacar una acción realizada por muchos programadores, lo que involucra la definición de identificadores de usuarios especiales o contraseñas que nadie conoce. A pesar de que son relativamente fáciles de codificar, y difíciles de descubrir por otros, estos mecanismos de acceso evaden los controles del ciclo de vida de desarrollo de sistemas en la organización. Estos mecanismos de acceso también evaden el proceso de petición normal de privilegios del usuario final y el proceso subsiguiente de autorización de parte de la gerencia. Estos mecanismos le pueden dar acceso a los programadores a una poderosa funcionalidad, aún si estos programadores no trabajan más para el empleador. Debido a que se encuentran fijos en el código, estos mecanismos no pueden ser eliminados o desactivados cuando un desarrollador abandona el empleo de un proveedor de software, a pesar de que se vuelvan muy conocidos. Asimismo, los violadores pueden utilizar estos mismos identificadores de usuario y contraseñas. Otra razón para proscribir dichos identificadores de usuario y contraseñas es que le dan control a uno o más desarrolladores sobre la seguridad del software cuando este control debe haberse transferido a la organización que utilizará el software que fue licenciado, alquilado o vendido. La referencia a la documentación del sistema se considera un impedimento. Si los desarrolladores se sintieran avergonzados por incluir un mecanismo especial de acceso en la documentación, probablemente éste no debería encontrarse en el sistema.

Políticas Relacionadas: “Burlado de los Controles de Acceso,” “Vías de Acceso en Software de Producción,” y “Acceso Físico de Trabajadores Cesados”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Controles de Acceso al Sistema de Computación

Política: Toda información sensible, crítica o valiosa residente en el computador debe tener controles de acceso en el sistema para garantizar que no sea divulgada en forma inapropiada, modificada o convertida en no disponible.

Comentario: Esta política requiere que únicamente la información que lo necesite será protegida con sistemas de control de acceso. Idealmente, las medidas de seguridad están diseñadas en forma consistente, de manera que la información esté protegida adecuadamente a donde quiera que viaje, sea quien sea el que la maneje o cualquiera sea la tecnología empleada y cualquiera sea la forma que tome. Esta política exige el uso de controles de acceso para soportar esa noción. La política asume que se ha adoptado un sistema de clasificación de datos. Las palabras "sensible", "crítica" y "valiosa" deben ser específicamente definidas por la gerencia antes de que esta política pueda ser aplicada en forma práctica. También es una buena idea definir los "controles de acceso al sistema". A pesar de que muchos sistemas operativos no incluyen controles de acceso, la mayoría de los sistemas operativos multiusuario incluyen la clase de controles de acceso requeridos por esta política. Para aquellos sistemas que carecen de software para soportar el control de acceso, se necesitarán paquetes de software suplementarios. Esta política también es relevante para los sistemas cliente-servidor, sistemas de computadores portátiles y asistentes personales digitales. Los sistemas remotos muy pequeños, como los buscapersonas alfanuméricos, pueden no ser capaces de soportar los controles de acceso deseados, en cuyo caso la organización debe decidir si acepta correr el riesgo o prohibir el manejo de información en dichos sistemas.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Funcionalidad de la Seguridad en las Aplicaciones del Negocio,” y “Arquitectura de Sistemas para Registro de Actividades”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Acceso a Material Adulto

Política: Antes de permitir el acceso a cualquier material que el público general considera inapropiado para los niños, todos los sistemas de la Empresa X deben emplear un sistema de control de acceso mediante verificación de la edad, aprobado por la gerencia de Seguridad Informática.

Comentario: Esta política informa al personal técnico acerca de las circunstancias en las que se requiere un sistema especial de control de acceso. Este sistema no es del tipo usual, el cual podría por ejemplo involucrar contraseñas dinámicas o fijas sino uno que verifique la edad del usuario. Esto podría involucrar simplemente dar un clic sobre un botón declarando que el usuario afirma que tiene al menos una determinada edad. Esto podría también involucrar el ingreso de un número legítimo de tarjeta de crédito que pueda ser confirmado en línea. También se puede utilizar como mecanismo para verificar la edad la capacidad de proveer un número legítimo de licencia de manejo. Esta política evita deliberadamente la referencia a una solución técnica específica. Esta política está impulsada por el creciente uso de Internet y el acceso a material para adultos de parte de los niños a través de Internet. La existencia de esta política puede servir como evidencia de la intención de la gerencia de restringir ciertos materiales únicamente a los adultos y está en conformidad con las leyes locales.

Políticas Relacionadas: “Recopilación de Información Personal de Menores” y “Almacenamiento de Información de Clasificación Mixta”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Separación de Actividades y Datos

Política: La gerencia debe definir los privilegios de los usuarios de forma tal que los usuarios ordinarios no puedan tener acceso o interferir en las actividades individuales o los datos privados de otros usuarios.

Comentario: Esta política evita que los gerentes de sistemas establezcan controles de acceso en sistemas multiusuario de forma tal que los usuarios puedan causar daño en los archivos de otros usuarios, revisar el trabajo de otros usuarios o exceder los privilegios que requieren para realizar su propio trabajo. Mucha de esta clase de daño por lo general no es intencional, debido a que podría ser forjada por un programa escrito por un usuario que altere los datos que pertenecen a otro usuario. Esta política prohíbe implícitamente compartir

un identificador de usuario y utilizar contraseñas que sean conocidas y utilizadas por varias personas. Esta política asume espacios de trabajo lógicos separados para cada usuario y está escrita de manera que es completamente consistente con ambientes de computación como los sistemas de conjuntos de programas, sistemas gerenciales, almacenes de datos o determinadas clases de sistemas de realidad virtual. Nada de lo mencionado en esta política prohíbe el uso de recursos compartidos como los que frecuentemente se encuentran en redes de área local, como por ejemplo los directorios públicos para almacenar archivos compartidos.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#)” y “[Separación de Tareas](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

6. Capacidad de Acceso de Usuarios

Política: Los usuarios no deben leer, modificar, borrar o copiar un archivo que pertenezca a otro usuario sin obtener permiso del Propietario del mismo.

Comentario: Esta política define los límites apropiados para los archivos mantenidos por los usuarios de computadores personales, quienes por lo general no poseen controles de acceso para sus archivos. No se hace mención a los computadores personales en la política debido a que también puede aplicarse a sistemas más grandes. Para éstos, esta política puede aplicarse siempre que los controles de acceso sean deficientes, o cuando se descubra una inconsistencia en los controles de acceso existentes. Esta política hace referencia a los Propietarios de la información que idealmente tomarán decisiones acerca del acceso a ciertos tipos de información. No obstante, para muchas clases de información, el Propietario es el usuario predeterminado en aquellos computadores personales en los que reside la información. Algunas organizaciones pueden desear cambiar la política de manera que se refiera al usuario de un sistema como un sustituto del Propietario de un archivo. La palabra "archivo" puede también generalizarse y convertirse en "colección de información".

Políticas Relacionadas: “[Mal Funcionamiento del Control de Acceso](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Privilegios Predeterminados de Usuario

Política: Sin la autorización específica por escrito de la gerencia, los administradores no deben conceder ningún privilegio a ningún usuario más allá del correo electrónico y de los procesadores de palabras.

Comentario: Esta política establece un grupo de privilegios del sistema que se les dará a todos los usuarios autorizados de manera que puedan comunicarse con otros usuarios y puedan realizar sus trabajos, más allá de los cuales se requerirá autorización. El grupo básico de privilegios puede por ejemplo otorgarse a todos los empleados que ingresan a la organización. Cuando se han definido suficientemente sus responsabilidades, necesitarán efectuar peticiones especiales para obtener más privilegios. Estas peticiones deben efectuarse utilizando formularios especiales que pueden ser enviados a través del correo electrónico o de formularios electrónicos. La idea detrás de esta política puede extenderse e incluir el establecimiento de privilegios por defecto de acuerdo con el cargo y privilegios por defecto por departamento. Pueden añadirse otros privilegios a la lista de privilegios por defecto. Por ejemplo, pueden añadirse la navegación por Internet y los programas de hojas de cálculo.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Comandos y Capacidades del Sistema

Política: Se debe presentar a los usuarios finales únicamente las capacidades y comandos del sistema para los cuales tienen privilegios.

Comentario: Esta política limita las escogencias de los usuarios finales a aquellas opciones para las que se les han otorgado privilegios. Esto hace que el uso del sistema sea más simple, más directo y además aumenta la seguridad. Si los usuarios no saben que no pueden hacer algo, será más difícil que soliciten esos privilegios. Esta política puede disparar una reducción marginal en los costos de administración de los controles de acceso. Esta política también evita que los usuarios curiosos traten de emplear capacidades y comandos para los cuales carecen de adiestramiento o autorización. Esta política establece claramente cuáles privilegios han sido autorizados y cuáles no, y puede ayudar a los administradores y diseñadores de sistemas a tomar decisiones apropiadas con relación al control de acceso. Esta política también diagnostica problemas en

los usuarios. Si una determinada opción no se muestra, significa que no se han otorgado todavía los privilegios. Esta política será aplicable únicamente al software desarrollado internamente. El software desarrollado por terceros generalmente no es modificable para que pueda estar conforme con esta política.

Políticas Relacionadas: "Privilegios Especiales en Sistema," "Mecanismo Único de Acceso," y "Restricción de Privilegios — Necesidad de Conocer"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Privilegios Sobre la Información de Producción

Política: Los privilegios del sistema que permiten la modificación de la información de producción de la Empresa X deben estar restringidos a las aplicaciones de producción.

Comentario: Los usuarios no deben ser capaces de cambiar los datos de producción a menos que dicha modificación se haga a través de software de producción bien definido y previamente aprobado. Por ejemplo, los empleados no deberían ser capaces de modificar las nóminas a menos que lo hagan a través de un proceso prescrito que incluya los controles de acceso dentro del sistema de pagos. Únicamente cuando este proceso se ha seguido, pueden aplicarse consistentemente la conexión, validación de las entradas de datos y demás controles. A los usuarios ordinarios no se les debe permitir el uso de editores de texto, depuradores de programas y demás herramientas poderosas que modifican directamente la información de producción. Siempre existirá la necesidad ocasional de determinado personal, como por ejemplo un grupo selecto de administradores de sistemas, que sea capaz de modificar directamente los datos de producción. Esto debe ser severamente restringido, supervisado, registrado y periódicamente revisado. Muchos sistemas operativos comerciales de computadores personales y redes de área local hacen que esta política sea difícil de implementar, a pesar de que se trata claramente de una tendencia emergente. Esta política puede ser implementada eliminando ciertos programas utilitarios como los compiladores y editores de texto. Esta es una práctica normal en los servidores comerciales en Internet.

Políticas Relacionadas: "Acceso a Comandos del Sistema Operativo" y "Modificación de la Información de Negocio de Producción"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10. Actualizaciones de la Base de Datos

Política: Las actualizaciones a las bases de datos de producción sólo podrán efectuarse a través de los canales establecidos que hayan sido autorizados por la gerencia.

Comentario: Esta política evita que el personal cause problemas operacionales que puedan interrumpir o interferir con el proceso de producción. Esta política prohíbe el uso de servicios que puedan evadir los controles de acceso, y vayan directo a la base de datos para modificar los datos allí almacenados. Esta política proporciona la base para tomar acciones disciplinarias en el caso de que el personal de programación de sistemas, administración de sistemas, operadores de sistemas de computación cometan actos abusivos. Quizás la manera más efectiva de implantar esta política es criptografiar los archivos de producción al igual que una base de datos.

Políticas Relacionadas: "Modificación de la Información de Negocio de Producción" y "Actualizaciones Automáticas de Software"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Aplicaciones de Producción Multiusuario

Política: Todas las aplicaciones de negocios de producción que respaldan a múltiples usuarios deben ser protegidas por un sistema de control de acceso autorizado por la gerencia de Seguridad Informática.

Comentario: Con algunos sistemas de control de acceso es posible establecer una lista de aplicaciones a las cuales el control de acceso no se aplique. Esto da lugar a una excepción que no es consistente con otros controles de acceso, y puede no estar tan bien protegida o registrada como otros controles de acceso. Esta política, dirigida primordialmente a administradores de sistemas, establece que todas las aplicaciones de negocios deben ser controladas utilizando sistemas normales de control de acceso y que estén autorizados. La política también se aplica a sistemas más pequeños. En los servidores departamentales y en otros sistemas más pequeños es donde existen comúnmente las aplicaciones sin control de acceso adecuado. Esta política también alerta al lector a preguntar cuáles son los sistemas de control de

acceso autorizados por la gerencia de Seguridad Informática. Esta repuesta la encontramos en una lista de productos normales y vendedores autorizados.

Políticas Relacionadas: “Actualización de Información de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Divulgación de Registro del Sistema y Seguimientos de Auditorías

Política: Los registros del sistema o rastros de auditoría de aplicaciones no deben ser divulgados a personas fuera del equipo de individuos que ordinariamente ven tal información para ejecutar su trabajo o investigar incidentes de seguridad informática.

Comentario: Esta política evita que los registros de sistemas y rastros de auditorías de aplicaciones sean divulgados a personas que no tienen una necesidad legítima de conocer tal información. Los administradores de sistemas u otros pueden pensar que los solicitantes tienen autorización o una razón legítima para ver la información, cuando en realidad no la tienen. Los hackers, espías industriales y otros utilizan la ingeniería social para convencer a los administradores de sistemas y a personal técnico de que ellos tienen una razón legítima para tener acceso a este tipo de información. De igual manera los gerentes departamentales pueden alegar que están realizando una investigación sobre el desempeño de un trabajador. Para evitar este tipo de abuso, esta política requiere que la persona que va a divulgar el registro o el rastro de auditoría haga contacto con la gerencia de Seguridad Informática.

Políticas Relacionadas: “Acceso a Registros” e “Investigaciones de Seguridad Informática”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

13. Acceso a la Información de las Aplicaciones de Producción

Política: El personal que desarrolla el software de aplicación del negocio no debe tener acceso a la información de producción, con la excepción de la información que sea importante para el software de la aplicación en la cual estén trabajando.

Comentario: Esta política limita el acceso a la información de producción de tal manera que el acceso se otorgue sólo para la información que el personal necesite para el desarrollo de su trabajo. Por ejemplo, si están trabajando en el desarrollo de un sistema nuevo de cuentas por cobrar, no necesitan acceso a la información de producción de cuentas por pagar. La política requiere que la gerencia implemente controles de acceso a un nivel de detalles que ellos no habían previamente especificado. Ellos pueden haber dado a todos los que contribuyeron al desarrollo, el acceso a toda la información de producción. Esta política apoya el principio de separación de tareas. A pesar de que puede ser más difícil de lograr en los sistemas de cliente-servidor, redes de área local, computadores personales y ambientes relacionados con sistemas pequeños, esta política no está restringida a sistemas de gran magnitud.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer,” “Separación de Tareas,” y “Acceso del Desarrollador a la Información de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

14. Información Confidencial de Terceros

Política: Toda la información confidencial o de propiedad confiada a la Empresa X por un tercero, debe ser protegida como si fuese información confidencial de la Empresa X, a menos que en un contrato se especifique lo contrario.

Comentario: En muchos casos las personas que manejan la información de terceros no tienen acceso a los contratos que definen los procedimientos convenidos para el manejo de la información encomendada a la Empresa X. Una forma expedita de vencer esta falta de información es utilizar el esquema de clasificación interna de datos en la organización receptora para designar cómo debe ser protegida la información, y de manera predeterminada esta política le asigna la clasificación de confidencial a toda esa información. La política se puede modificar para designar un Propietario de información interno o un patrocinante de la Empresa X, quien posteriormente le asignará una etiqueta de clasificación de datos consistente con un esquema de clasificación de datos internos. Es recomendable en todo convenio donde se va a compartir información, emplear las clasificaciones y procedimientos de seguridad informática existentes.

Una variación a esta política requeriría que la información de terceros incluya una notificación designando el verdadero Propietario de la información.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

15. Acceso a la Información Personal

Política: Toda la información de clientes que identifique números de tarjetas de crédito, referencias de crédito o cédulas de identidad, debe ser sólo accesible al personal de la Empresa X que necesita ese acceso para hacer su trabajo.

Comentario: Esta política deja claro que la información financiera y personal sobre los clientes sólo puede ser utilizada por personas que tenga una necesidad genuina de esta información. Es la disponibilidad general de esta información lo que hace más fácil los robos de identidad. Esta política es deliberadamente silente con respecto a los mecanismos utilizados para restringir el acceso. Esto le da a gerencia flexibilidad para escoger los controles que mejor logren el objetivo definido en esta política. La política puede ser ampliada a empleados y otros grupos de personas para quienes la organización mantiene registros. La política puede adicionalmente ser útil para relaciones públicas como una indicación de la posición proactiva de la organización.

Políticas Relacionadas: “[Eliminación de la Información de Pago](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

16. Acceso al Almacén de Datos

Política: El acceso al almacén de datos debe ser restringido a la gerencia media y alta de la Empresa X.

Comentario: El acceso al almacén de datos debe ser restringido sólo a la gerencia media y alta o a un grupo selecto de trabajadores autorizados, como los planificadores estratégicos. Un enfoque alternativo sería el hacerlo accesible sólo a través de un intermediario, como un asistente de investigaciones, quien pudiera también hacer una evaluación de la necesidad genuina del solicitante a la información solicitada. Esta forma intermedia de implantar la política, aunque

ineficiente, tiene la ventaja de que se aplicará consistentemente. Esta política debe ser distribuida sólo a los administradores de sistemas y otros que otorguen privilegios de sistemas. Esta política puede adaptarse para ser utilizada en una variedad de colecciones de información incluyendo bases de datos muy grandes.

Políticas Relacionadas: “[Restricciones a la Recopilación de la Información](#)” y “[Etiquetado de Clasificación Múltiple](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Diseminación Secundaria de la Información Secreta

Política: La información secreta debe ser divulgada sólo cuando se haya obtenido la autorización explícita del Propietario, y ninguna persona a quien se haya otorgado el acceso a información secreta no debe divulgarla a ninguna otra persona.

Comentario: Esta política evita que personas que tengan información secreta la comuniquen a otras personas sin el permiso del Propietario de la información. Las personas en poder de información secreta no heredan el derecho de diseminarla. Debido a que esta noción es contraria a la práctica común, es necesario tener una política específica. Esta política asume que el término "Propietario de la información" ha sido previamente definido. La palabra "secreta" pudiera ser reemplazada por "sensible" o por un conjunto de clasificaciones de información sensible específica usada por la organización. La política asume que el término "secreta" ha sido definido.

Políticas Relacionadas: “[Propiedad de la Información](#),” “[Clasificación de Datos en Cuatro Categorías](#),” “[Acuerdos de Confidencialidad](#),” y “[Manejo de Información Sensible](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

18. Acceso a Información Sensible o Valiosa

Política: El acceso a la información sensible o valiosa de la Empresa X debe ser otorgado sólo después de obtenerse la autorización expresa de la gerencia.

Comentario: Esta política restringe el acceso a los datos sensibles y valiosos de la Empresa X, no permitiendo que las personas tengan acceso, a menos que hayan

obtenido aprobación explícita de la gerencia. Esta política desanima a los trabajadores en el sentido de compartir dicha información con otros trabajadores o terceros sin la aprobación de la gerencia. La política es generalmente una política de alto nivel bajo la cual se pueden añadir varias políticas más detalladas relacionadas con controles de acceso. En lugar de utilizar el término "autorización de la gerencia" la política se pudiera referir a "autorización del Propietario de la información". También se pueden usar los términos "secreta", "confidencial" y "privada". A pesar de que esta política puede ser utilizada sin tener un sistema interno de clasificación de datos, es más efectiva cuando las palabras "sensible" y "valiosa" han sido definidas en otra política.

Políticas Relacionadas: "Clasificación de Datos en Cuatro Categorías" y "Restricción de Privilegios — Necesidad de Conocer"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

19. Acceso a la Información Secreta

Política: El acceso a la información secreta se debe otorgar solamente a personas específicas, no a grupos de personas.

9.06.02 Aislamiento de Sistemas Sensibles

1. Servidores para Aplicaciones Críticas

Política: A menos que las consideraciones técnicas indiquen que sería excesivamente costoso, los servidores de producción críticos deben ser máquinas dedicadas a un propósito, ejecutando sólo una aplicación.

Comentario: Esta política aísla las aplicaciones críticas de manera que tengan sus propios servidores. Esto reducirá las oportunidades en las cuales el servidor se caiga debido a conflictos e incompatibilidades entre varios paquetes de software. Existen a veces combinaciones asincrónicas de eventos del sistema que pueden causar que los sistemas de operaciones se tranquen. Por ejemplo, una aplicación puede tener un error de programación que cause un desbordamiento de la memoria intermedia. Si esa aplicación tuviera su propio servidor, sólo esa máquina se desestabilizaría, pero si se hospedara en un servidor compartido, todas las aplicaciones en esa máquina se caerían. De tal manera que

Comentario: Esta política requiere que la gerencia tome decisiones persona por persona cuando esté otorgando acceso a los tipos de información más sensibles. Si el acceso es otorgado a grupos de personas, inevitablemente habrá un acceso mayor de lo necesario. Igualmente, si el acceso se otorga a un grupo, es mucho más difícil establecer una responsabilidad. Cuando se decide otorgar acceso a información sensible, la gerencia debe considerar el tiempo que la persona tiene con la organización, sus responsabilidades, problemas disciplinarios, potenciales conflictos de intereses, el grado de lealtad a la organización y todo otro asunto relacionado. Esta política apoya la práctica de tener un identificador de usuario para cada individuo. Esta política puede ser ampliada a todos los tipos de información sensible. La política asume que la palabra "secreta" ha sido definida en otra política.

Políticas Relacionadas: "Restricción de Privilegios — Necesidad de Conocer," "Identificador Unico de Usuario y Contraseña Obligatorios," "Clasificación de Datos en Cuatro Categorías," y "Acceso a Información Sensible o Valiosa"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

esta política está dirigida a incrementar el tiempo de funcionamiento y la confiabilidad de los servidores, para simplificar la administración del sistema, para facilitar la vigilancia del desempeño del sistema y para mantener el número de maneras en que un servidor se puede ver comprometido.

Políticas Relacionadas: "Dispersión de Sistemas Computacionales" y "Computadores para Cortafuegos"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Aislamiento de Sistemas con Información Secreta

Política: Los sistemas de computación de la Empresa X que contienen información secreta no deben estar conectados con ninguna red u otro computador.

Comentario: Esta política evita la divulgación no autorizada de información sensible. Sabiendo que los controles de acceso a redes son poco confiables, algunas organizaciones han decidido prohibir toda conexión con redes, para que la información no sea divulgada inapropiadamente. Esta política conservadora puede en muchos casos ser remplazada por una política que requiera cifrados sólidos cuando la información secreta no se esté utilizando. Algunas organizaciones prohíben cualquier otra aplicación en el computador involucrado, convirtiéndolo así en un computador dedicado. Con la prisa por interconectar virtualmente todos los sistemas dentro de las organizaciones, algunos gerentes querrán

mantener fuera de la red algunos sistemas de alta seguridad, particularmente Internet. Esto no causará problemas mayores en lo que se refiere a la ejecución del trabajo. Cuando sea necesario transferir datos desde un sistema de alta seguridad a uno de más baja seguridad, se pueden utilizar discos flexibles o cualquier otro medio de almacenamiento en lugar de la red.

Políticas Relacionadas: “[Interconexión de Sistemas](#)” e “[Información Secreta en la Web](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

9.07 Monitoreo del Acceso y Uso del Sistema

9.07.01 Registro de Eventos

1. Registros en Sistemas y Aplicaciones Sensibles

Política: Todos los sistemas de aplicaciones que manejen información sensible de la Empresa X deben generar registros que capten toda adición, cambio y eliminación de dicha información.

Comentario: Esta política ofrece la posibilidad de responsabilizarse por los cambios efectuados a la información sensible, tales como registros de personal, planes estratégicos y especificaciones de diseños. Por ejemplo, la base de datos de nómina debe tener un registro asociado que indica quién actualizó las cantidades y cuándo. Este tipo de información es de mucha ayuda cuando se trate de investigar y corregir problemas como errores y desfaldos. Esta política indica cuáles aplicaciones deben tener registros asociados o rastros de auditoría. Los elementos del registro de datos tendrán que ser determinados caso por caso. El alcance de la política puede ser fácilmente ampliado para incluir información sensible, crítica, y valiosa de la Empresa X. En algunos casos, el sistema operativo, los sistemas de aplicaciones o el sistema de base de datos de la gerencia son capaces de captar suficiente información de registro.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Contenido de Registros en Aplicaciones de Producción

Política: Todos los sistemas de computación que manejen sistemas de aplicaciones de producción de la Empresa X deben incluir un registro que contenga, como mínimo, actividades de sesiones de usuarios incluyendo su identificador de usuario, fecha y hora de inicio y cierre de la sesión, aplicaciones utilizadas, cambios a los archivos críticos de los sistemas de aplicaciones, adiciones y cambios a los privilegios de los usuarios e inicios y cierres de sistemas.

Comentario: Esta política proporciona una colección de registros de datos que pueden estar disponibles en todo sistema interno que ejecute una aplicación de producción. Esta información no sólo ayudará en los esfuerzos por resolver un problema y restablecer la operación, sino que también es valiosa para las investigaciones sobre ataques de penetración al sistema y fraudes. Mediante la normalización de unos requerimientos mínimos de registro, una organización puede ayudar a los administradores de sistemas a tomar decisiones para configurar un sistema. Con una política como ésta se pueden colocar las bases para un sistema integrado multimáquina de detección de intrusiones.

Políticas Relacionadas: “[Registro de Eventos Importantes de Seguridad](#)” y “[Registros en Sistemas y Aplicaciones Sensibles](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Registro de Eventos Importantes de Seguridad

Política: Los sistemas de computación que manejen información sensible, valiosa o crítica, deben registrar de forma segura todos los eventos importantes relativos a la seguridad incluyendo, sin limitantes, los intentos de deducir la contraseña, utilizar privilegios no autorizados, y cambios al software de aplicación de producción y al software del sistema.

Comentario: Esta política especifica cuáles sistemas de computación deben tener registros de sistemas que reflejen eventos importantes de seguridad. Es particularmente apropiado para computadores personales, estaciones de trabajo, servidores de redes de área local, sistemas cliente-servidor y sistemas pequeños similares que no tienen registros adecuados. Será necesario especificar en la política exactamente constituye un evento importante de seguridad. Otra manera de manejar esto es la de indicar que la gerencia de Seguridad Informática determinará exactamente qué es lo que constituye un evento importante de seguridad. La política sólo requiere registros para sistemas que manejan información sensible, valiosa o crítica. Debido a que hace referencia a información confidencial, valiosa o crítica, esta política se apoya implícitamente en una política de clasificación de datos.

Políticas Relacionadas: “[Clasificación de Datos en Cuatro Categorías](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Registro de Intentos de Acceso

Política: Deben registrarse todos los intentos de los usuarios por iniciar la sesión y conectarse con los sistemas informáticos de producción de la Empresa X, sin importar si fueron exitosos o no.

Comentario: Esta política crea un amplio conjunto de registros de sistemas de operación a lo largo de todos los sistemas internos de información de producción que puedan ser utilizados con propósitos investigativos o administrativos. Los registros también son una entrada muy importante para los sistemas de detección de intrusos en computadores, porque pueden automáticamente alertar al personal técnico sobre un ataque en pleno desarrollo. Una cadena de intentos incorrectos de inicio de sesión sería evidencia de un ataque para adivinar la contraseña o de un usuario que necesita

adiestramiento adicional. Estos registros de sistemas captarán el identificador de usuario, hora y fecha, el puerto que utilizó y si el intento de inicio de sesión fue exitoso. Esta política está restringida a sistemas informáticos de producción de tal forma que los registros de sistemas no serán necesarios en computadores de escritorios y otros no críticos para el negocio.

Políticas Relacionadas: “[Contenido de Registros en Aplicaciones de Producción](#)” y “[Sincronización del Reloj](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Registros de Eventos de Seguridad Iniciados Por Usuarios

Política: Se debe llevar uno o más registros que rastreen las actividades importantes de seguridad de un usuario específico por un período de tiempo razonable.

Comentario: Esta política especifica que toda la actividad importante de seguridad iniciada por los usuarios debe ser registrada y retenida por un período adecuado. Esta información es útil a las personas en la administración de seguridad, operaciones de computación y auditorías internas. La información también sirve como un elemento disuasivo ante abusos y es muy importante para que el uso de soporte técnico cuando esté investigando un problema. La política hace referencia a actividades importantes de seguridad, como los cambios que hace el usuario para lograr acceso a los archivos privilegiados o los cambios de las contraseñas secretas. Si la política fuese sólo distribuida a la gerencia y al personal técnico, la política podría incluir una definición específica de actividades importantes de seguridad. Puede ser apropiado mantener el término “actividades importantes de seguridad” ambiguo para que la gerencia de sistemas locales pueda interpretarlo a conveniencia. Los gerentes de sistemas locales pueden determinar que las aplicaciones y las actividades de sistemas son importantes para la seguridad, o pueden alternativamente determinar que sólo las actividades de sistemas son importantes para la seguridad.

Políticas Relacionadas: “[Consentimiento para Acciones Cuestionables en los Sistemas](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Registros de Acceso a Información Privada

Política: Se debe registrar la identidad de cada usuario que acceda a la información privada contenida en los sistemas informáticos de la Empresa X.

Comentario: Esta política clarifica los tipos de información que se deben guardar en los registros y en los rastros de auditoría. Este tipo de información generalmente se reproduce en un sistema de aplicaciones de rastros de auditoría en vez de un registro del sistema. Esta política es útil en cualquier organización donde la privacidad es un principio. Esta política también es útil en el caso de identificaciones fraudulentas, o en cualquier investigación que busque identificar cómo cierta información privada llegó a manos de personas no autorizadas.

Políticas Relacionadas: “Manejo del Registro Personal” y “Registros en Sistemas y Aplicaciones Sensibles”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

7. Período de Retención de Registros

Política: Los registros computarizados que contengan eventos importantes de seguridad se deben retener como mínimo tres meses, y dentro de ese tiempo se deben proteger para que no puedan modificarse y que sólo puedan leerlos las personas autorizadas.

Comentario: Esta política especifica el período de retención para registros y la necesidad de almacenamiento seguro para los mismos. La política puede ser ampliada para definir explícitamente cuáles eventos son considerados importantes para la seguridad. No hay nada especial sobre el período de tres meses. El período de retención variará por industria, jurisdicción y la información involucrada. El asesor legal interno y personal de la gerencia de registros deben ser consultados sobre el período adecuado para retener dichos registros. El período de retención para transacciones de negocios será generalmente más largo que el período de retención de eventos importantes de seguridad.

Políticas Relacionadas: “Registros del Sistema de Control de Acceso” y “Retención de Registros de Privilegios de Control de Acceso”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Remoción de Registros de Computadores Accesibles desde Internet

Política: Los registros de sistemas y aplicaciones contenidos en computadores accesibles por Internet deben ser movidos por lo menos diariamente a otras máquinas que no sean directamente accesibles desde Internet.

Comentario: Esta política resguarda la integridad de los registros. Si los registros se mantienen por un tiempo prolongado en máquinas accesibles desde Internet, las probabilidades de que los hackers y otros no autorizados los modifiquen aumentan significativamente. La necesidad de proteger los registros es mayor si contienen información de pagos como los números de las tarjetas de crédito, o si los registros contienen información privada como números de teléfonos. La transferencia diaria a máquinas más seguras simplemente significa descargar los registros a una máquina que esté detrás de otro cortafuego. Puede significar que se graben los registros en cinta y se almacenen fuera de línea. En vez del proceso descrito en esta política, una opción más segura es no guardar ningún registro en máquinas accesibles por Internet. Esto puede involucrar la transferencia de información en tiempo real, evento por evento, hacia otra máquina que esté detrás de otro cortafuego.

Políticas Relacionadas: “Información de Registro del Cliente,” “Desactivación, Cambio o Eliminación de Registros,” y “Retención de Registros de Privilegios de Control de Acceso”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Retención de Registros de Privilegios de Control de Acceso

Política: Los registros computarizados que reflejen los privilegios de acceso de cada usuario en los sistemas multiusuario y redes de la Empresa X se deben conservar de manera segura por un período razonable de tiempo.

Comentario: Como parte de una investigación de un delito de computación, la gerencia querrá determinar el autor de ciertas acciones en un sistema o red. Esta política especifica que los registros sobre los privilegios de control de acceso de usuarios se capten y mantengan por un período de tiempo. Algunas organizaciones podrán explícitamente establecer un período de retención de registros, como por ejemplo tres meses, en esta política. Otras organizaciones dejarán el período

abierto para que la gerencia local lo determine. En esta política, se hizo referencia a sistemas multiusuario porque la identidad del perpetrador de un acto abusivo es un problema menor en un computador personal o una estación de trabajo. Igualmente, estos sistemas más pequeños son menos propensos a tener cualquier tipo de registro que refleje los privilegios de los usuarios. La política puede ser ampliada para incluir estos sistemas más pequeños. Una simple omisión de la palabra "multiusuario" puede ser suficiente. La política, tal como está escrita, es importante para los sistemas de comunicación de voz y de datos.

Políticas Relacionadas:“[Otorgamiento de Privilegios del Sistema](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

10. Arquitectura de Sistemas para Registro de Actividades

Política: El software de sistemas de aplicaciones o base de datos de la gerencia debe conservar registros de las actividades de los usuarios y estadísticas relacionadas a esas actividades que permitan identificarlas y emitir alarmas que reflejen algún acontecimiento sospechoso del negocio.

Comentario:Consideren una compañía que otorga tarjetas de crédito y que mantiene un registro del número de transacciones de cada tarjeta por semana. Si esta estadística excede de manera notable la historia de uso habitual, puede indicar que la tarjeta ha sido robada y se está utilizando para efectuar compras fraudulentas. Esta política especifica dónde se debe mantener cierto tipo de registros, en un sistema de operaciones de computador, sistema operativo de redes, software de control de acceso, software de sistemas de la base de datos, o en el software de aplicaciones. Esta política indica que los acontecimientos de negocios, como los montos cargados a una tarjeta de crédito, se deben captar en registros y conservarse en un sistema de aplicaciones o administración de base de datos. La organización puede especificar si otros tipos de información, como los cambios en los privilegios de usuarios, también deben ser registrados. Esta política es una instrucción técnica de diseño de sistemas, y forma parte frecuente de la arquitectura de seguridad informática. Hoy en día muchas organizaciones están desarrollando un plan, o arquitectura, que especifica dónde serán soportados los controles críticos, como los registros.

Políticas Relacionadas:“[Controles de Acceso al Sistema de Computación](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

11. Registros de Auditoría en los Sistemas

Política: Los registros de los eventos importantes de seguridad en computación deben proporcionar datos suficientes como para apoyar auditorías amplias de la eficacia y cumplimiento de las medidas de seguridad.

Comentario:Los auditores externos no dependerán de los registros financieros de la organización si no hay suficiente evidencia de que los controles están funcionando correctamente. Si éste fuese el caso, significa que los auditores externos tendrán que efectuar otras pruebas de los registros para verificar su exactitud, quizás incurriendo en honorarios adicionales. Similarmente, sin suficiente información de registro, los auditores internos tampoco podrán efectuar su trabajo, lo cual incomodará a la gerencia con respecto a la seguridad de los sistemas. Esta política garantiza que los registros proporcionarán suficiente información para permitir que la auditoría interna y la externa procedan sin costos excesivos. Los registros efectivos también pueden ser de ayuda en la resolución de problemas operacionales, como la determinación de la causa de la caída del sistema. Esta política es adicionalmente útil porque alerta a la gerencia para que considere exactamente cuáles tipos de datos deben ser captados en los registros. Algunas organizaciones podrán ampliar esta política para incluir los datos necesarios para acciones legales o acciones disciplinarias al personal.

Políticas Relacionadas:“[Revisión de los Controles de los Sistemas Informáticos — Interno](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

12. Registros Espejos Remotos

Política: Todos los sistemas informáticos de producción de la Empresa X que sean accesibles desde cualquier red externa deben emplear registros espejos remotos.

Comentario:Esta política requiere un cierto diseño que es popular con los comerciantes de Internet. Este diseño de sistemas seguros involucra la grabación remota de los registros del sistema en otra máquina, preferiblemente con un sistema operativo diferente. El uso de un sistema operativo diferente significa que un intruso

tendrá mayores dificultades para ingresar en el sistema del registro remoto. Esta dificultad impondrá una demora que será suficiente para que el sistema de detección de intrusos alerte a las autoridades de la presencia de un intruso. La política está basada en la suposición que una de las primeras cosas que un intruso hace cuando compromete a una máquina es apagar, modificar o borrar el registro del sistema. Estas acciones pueden ocultar la huella del intruso, pero si el registro del sistema está almacenado en otra máquina, es más difícil alterarlo. Para el más alto nivel de seguridad, los registros remotos se pueden cifrar para evitar la divulgación no autorizada, un cambio no detectado, y también almacenarlos en modo sólo escritura para evitar cualquier modificación.

Políticas Relacionadas:“Registros de Aplicaciones Críticas” y “Desactivación, Cambio o Eliminación de Registros”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

13. Rotación y Archivado de Registros del Sistema

Política: Se debe emplear un proceso formal de rotación y de archivo de los registros en todos los sistemas de seguridad periféricos de la red y en los servidores multiusuario de producción.

Comentario:Esta política es para que los administradores de sistemas establezcan y sigan un proceso formal de rotación y archivado de los registros de los sistemas. En algunas organizaciones, los administradores de sistemas no piensan en los registros hasta que han excedido su capacidad en el disco. Los archivos de registros muy grandes son difíciles de manejar, de mover de máquina a máquina y de registrar en caso de necesitarse un evento específico. Tener unos archivos de registros razonablemente grandes que se roten hacia distintos medios de almacenamiento, mejora estas actividades.

9.07.02 Monitoreo del Uso del Sistema

1. Registros de Actividad de Identificadores de Usuarios Privilegiados

Política: Todas las actividades de creación, eliminación y cambio de privilegios en identificadores de usuario ejecutadas por administradores de sistemas y otros con

Políticas Relacionadas:“Copias Múltiples de Respaldo”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

14. Conciencia del Usuario Sobre Registros de Violaciones de Seguridad

Política: Los usuarios deben estar debidamente informados sobre las acciones que constituyen infracciones de seguridad y que tales infracciones serán registradas.

Comentario:Esta política requiere que todos los usuarios estén debidamente informados sobre las acciones que constituyen infracciones de seguridad. Para desanimar a los usuarios de involucrarse en estas acciones, se les debe informar que sus actividades serán registradas. Será muy difícil implementar acciones disciplinarias si los usuarios no han sido informados y no entienden que es lo que se espera de ellos. Si la política va a ser distribuida a los usuarios, puede incluir palabras indicando que "debido a las infracciones, los usuarios están sujetos a acciones disciplinarias que incluyen la terminación de la relación laboral y juicios penales". Esta política se puede acompañar con una explicación de ejemplos específicos de infracciones de seguridad. Estas infracciones incluirían los intentos de comprometer los controles tratando de adivinar la contraseña, cambios en los controles de acceso al sistema, hacerse pasar por otro usuario, y otras acciones, como por ejemplo desestabilizar el sistema.

Políticas Relacionadas:“Herramientas de Monitoreo de Sistemas”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

identificadores de usuarios privilegiados, deben ser registradas de manera segura y reflejadas en reportes periódicos a la gerencia.

Comentario:Esta política especifica cuáles actividades asociadas con el identificador de usuario privilegiado, necesitan registrarse y reflejarse en reportes periódicos a

la gerencia. La gerencia a veces no está clara sobre esto, y como resultado, se generan insuficientes registros y reportes a la gerencia. En ausencia de instrucciones específicas, los administradores de sistemas y otros tienden a apagar los registros y reportes para liberar espacio en disco. Una variación de esta política involucraría la adición de otra frase requiriendo que los Propietarios de sistemas, Propietarios de información u otros responsables por el sistema correspondiente, revisen los reportes de gerencia sobre las actividades de los identificadores de usuarios privilegiados. Las palabras "registradas de manera segura" implican que los administradores de sistemas y otros usuarios privilegiados, no pueden fácilmente cambiar o eliminar entradas en el registro.

Políticas Relacionadas: "[Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema](#)" y "[Registro de Inhabilitaciones](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Capacidad de Reconstrucción de Cambios en Producción

Política: Todas las actividades de los usuarios que afecten la información de producción, deben poder ser reconstruibles desde los registros.

Comentario: Esta política garantiza que todos los errores, cambios fraudulentos y otras modificaciones impropias a la información de producción, pueden ser rápidamente detectados y corregidos. Por ejemplo, en el evento que la caída del sistema dañe una base de datos de producción, tales registros serán el instrumento para reconstruir la base de datos partiendo de una copia anterior. En este caso, se pueden utilizar fotos de la base de datos que muestren imágenes antes y después. En esta política se enfatiza la capacidad de reconstrucción de datos y en preservar y ampliar su integridad.

Políticas Relacionadas: "[Registros de Eventos de Seguridad Iniciados Por Usuarios](#)," "[Transacciones Distintas a Producción](#)," "[Ordenes para Cambiar Registros](#)," y "[Notificación de Falla en los Controles de la Integridad](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Registro de Cada Tecla Presionada

Política: Toda actividad con identificador de usuario privilegiado en los sistemas de producción de la Empresa X debe ser registrada con registros de teclas pulsadas.

Comentario: Esta política requiere que se activen registros intensivos para identificadores de usuarios privilegiados en los sistemas de producción. Cada tecla presionada por estos usuarios privilegiados se registrará de tal manera que todas las acciones puedan ser reconstruidas de manera precisa. Esta política es disuasiva contra abusos de la capacidad propia del identificador de usuario privilegiado. La política también ordena registros extensivos que pueden ser de utilidad en investigaciones o demandas de crímenes de computación, o solamente tratando de averiguar lo sucedido. Hay un tipo de registro más intenso que involucra no sólo las pulsaciones de teclas, sino también las pulsaciones del ratón. En ambientes de la más alta seguridad, ambos tipos de información se pueden registrar para identificar los usuarios privilegiados. El registro de pulsaciones de teclas sólo es aplicable a identificadores de usuarios privilegiados debido a las limitaciones del espacio en el disco, pero en ambientes de muy alta seguridad como los salones de transferencias cablegráficas de un banco, puede ser ampliada a todos los identificadores que se encuentran en máquinas de producción. Esta política garantiza que el registro de pulsaciones de tecla no puede ser inhabilitado fácilmente por el identificador de un usuario privilegiado. Esto se puede lograr haciendo que el software de registro se ejecute en un sistema de computación diferente al que está monitoreando.

Políticas Relacionadas: "[Mensaje de Advertencia en Inicio de Sesión](#)" y "[Registros en Sistemas y Aplicaciones Sensibles](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema

Política: Las órdenes privilegiadas emitidas por operadores de sistemas de computación se deben rastrear hasta personas específicas a través del uso de registros amplios.

Comentario: Esta política es particularmente importante para servidores, mini-computadores y mainframes, donde más de un operador pueden iniciar ciertas órdenes. La intención de esta política es

mantener la responsabilidad y rastreo de todas las órdenes privilegiadas del sistema que se emitieron. La política no está dirigida a sistemas pequeños como computadores personales, en las cuales no se designan operadores específicos. En los ambientes que necesitan alta seguridad, la política puede ser aplicada a pequeños sistemas o sistemas que contengan información particularmente sensible, valiosa o crítica. Esta política instruye a la gerencia de sistemas a mantener registros de todas las órdenes y una indicación de quién las emitió. Esta política y los controles utilizados para implantarla, sirven como elemento disuasivo ante actos abusivos. Estos registros también proporcionan información que puede ser útil para acciones disciplinarias o procedimientos legales. Más importante aún, los registros de comandos del sistema privilegiado pueden ser una herramienta para resolver y comprender problemas en el sistema. Más allá de los operadores del sistema computarizado, la política se puede ampliar para incluir otras personas que típicamente tienen privilegios especiales, como los administradores de seguridad de informática, auditores internos, programadores de sistemas y administradores de redes de área local. La definición de "órdenes o comandos privilegiados del sistema" puede ser incluida en la política o dejadas para que la gerencia del sistema la determine.

Políticas Relacionadas: "Acceso a Comandos del Sistema Operativo" y "Registros de Actividad de Identificadores de Usuarios Privilegiados"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Registro de Contraseñas

Política: Las contraseñas no cifradas no deben ser incluidas en los registros del sistema.

Comentario: Esta política evita que las contraseñas sean divulgadas a los operadores de los computadores, administradores del sistema y otros que no tengan autorización para ver las contraseñas de los usuarios. Si estos técnicos pudieran ver las contraseñas de los usuarios, sería una infracción de un procedimiento fundamental al diseño de sistemas de contraseñas fijas. Específicamente, para poder tener la responsabilidad del identificador de usuario y su contraseña relacionada, sólo el usuario involucrado debe conocer su contraseña. Si los registros graban las contraseñas, entonces el personal técnico que revisa los registros, descubrirían las contraseñas de otros usuarios, y con esta información pueden personificar a otros usuarios. Esta política inclusive prohíbe el registro de contraseñas incorrectas,

ya que esto puede permitir que cualquiera, al revisar el registro, utilice técnicas de deducción para determinar la contraseña correcta. El registrar contraseñas con cifrado es sin embargo permitido y puede ser requerido en ambientes de alta seguridad. Las contraseñas cifradas pueden ser descifradas por un grupo restringido de especialistas de seguridad con el propósito de obtener información adicional que pueda ser de ayuda en una investigación.

Políticas Relacionadas: "Información de Inicio de Sesión" y "Revisión de Registros de Operadores de Computadores"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Controles para Modificaciones de los Registros del Sistema

Política: Todos los sistemas informáticos de producción de la Empresa X, deben utilizar sumas de verificación criptográficas para proteger los registros del sistema.

Comentario: Esta política garantiza que los cambios o eliminaciones de registros de sistemas no autorizados serán evidentes inmediatamente. Una de las primeras cosa que los hackers y otros intrusos hacen cuando ganan acceso al sistema es inhabilitar el registro del sistema. Mientras los controles dictados por esta política no detectan que un registro ha sido apagado, sí alertarán al hecho de que un registro se ha manipulado, y esto se utilizará como entrada al sistema para la detección de intrusos. Tales sumas de verificación criptográficas están disponibles en software comercial y compartido. Estos métodos de sumas de verificación involucran una dependencia de serial de datos de manera que la modificación de solo un dígito causaría una alarma inmediata. Debido a que la criptografía esta involucrada, esta política introduce la necesidad de un proceso clave de gerencia. Sólo porque se utilizan sumas de verificación criptográficas para detectar modificaciones y eliminaciones no quiere decir que el registro completo tenga que ser criptografiado. La utilización de un proceso de criptografía sólo para sumas de verificación de registros tiene menos impacto en el desempeño del sistema. Una firma digital o la aplicación de un algoritmo de sintetización de mensajes (hash) aplicado al registro como un todo se puede utilizar en vez sumas de verificación criptográfica para obtener casi el mismo resultado.

Políticas Relacionadas: "Sistemas de Gestión de Claves de Cifrado," "Sistemas de Detección de Intrusos," y "Desactivación, Cambio o Eliminación de Registros"

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

7. Desactivación, Cambio o Eliminación de Registros

Política: Los mecanismos para detectar y registrar acontecimientos computarizados de seguridad, deben ser resistentes a intentos de desactivar, cambiar o eliminar el software de registro y los registros.

Comentario: La efectividad de los registros es dependiente de los mecanismos utilizados para proteger la integridad de los registros y los mecanismos usados para generar los registros. Si un programador de sistemas fuese capaz de activar o desactivar un registro, esto le permitiría efectuar una acción que no aparecería en el registro. Esta política informa al personal técnico que los controles de acceso adecuados deben estar activos para proteger tanto al registro como a los mecanismos que los generan. Algunas organizaciones pueden añadir más palabras a esta política indicando que todos los cambios al sistema de registros deben ser también registrados. Los lectores pueden considerar una variedad de mecanismos para proteger los registros incluyendo sistemas operativos basados en controles de acceso, cifrado, firmas digitales, algoritmos de sintetización de mensajes (hash) y códigos de autentificación de archivos. En algunos casos los registros son mantenidos en una máquina separada que utiliza un sistema operativo diferente.

Políticas Relacionadas:“[Cifrado en Medios de Respaldo](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

8. Medios de Almacenamiento de Sistemas de Producción

Política: Los sistemas de producción conectados a Internet deben almacenar todos los registros del sistema de producción en medios de almacenamiento que no se puedan cambiar una vez creados.

Comentario: Esta política evita los posibles cambios que se puedan realizar a los registros del sistema. El sistema de almacenamiento escriba-una-vez-lea-muchas-veces (WORM) puede ser utilizado para grabar irreversiblemente lo ocurrido en un

computador de producción. Este enfoque no graba lo ocurrido si las facilidades de inicio de sesión están desactivadas, pero el hecho de que las actividades de inicio de sesión fueron desactivadas aparecerá en los registros. Esta política es recomendada para generar registros confiables que pueden ser admitidos en juicios.

Políticas Relacionadas:“[Modificación de la Información de Negocio de Producción](#),” “[Archivos Críticos de Respaldo](#),” y “[Respaldo de Información Crítica](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

9. Protección de Registros del Sistema

Política: Todos los registros de sistemas computarizados de producción deben estar protegidos con firmas digitales y números en secuencia de entradas al registro, y deben también ser automáticamente monitoreados en busca de descensos bruscos en tamaño, fallas de firmas digitales y vacíos en la secuencia de entradas de registros.

Comentario: Esta política requiere que aumenten las medidas de control de los sistemas de producción que detectarán intromisiones en el registro del sistema. Una de las primeras cosas que los intrusos hacen cuando obtienen acceso no autorizado a un sistema es desactivar, eliminar o cambiar el registro del sistema. Esta política garantiza que los sistemas de registros de producción detectarán estas actividades, y seguidamente notificarán a quienes están capacitados para remover al intruso del sistema involucrado. Muchos sistemas operativos no incluyen códigos para ejecutar las funciones definidas en la política, y con frecuencia se requiere un software adicional. Los controles definidos en esta política garantizan que un sistema de detección de un intruso o sistema de gerencia de redes estará activo. Si una organización va a categorizar sus máquinas por necesidades de seguridad, las palabras “sistema computarizados de producción” en la política pueden ser remplazadas o aumentadas por las palabras “servidores de infraestructura y periferia de redes”.

Políticas Relacionadas:“[Transacciones de Entrada en Producción](#)” y “[Registros Espejos Remotos](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Altos

10. Acceso a Registros

Política: Todos los registros de sistemas y aplicaciones deben estar protegidos y sólo se permite el acceso a personas que tengan necesidad de conocer la información.

Comentario: Esta política limita el acceso a los registros de aplicaciones y sistemas, a las personas que tienen una necesidad genuina de tener dicho acceso. El acceso de personas no autorizadas puede revelar identificadores de usuarios, transacciones específicas y otra información que puede ser vital en fraudes, saboteo, espionaje industrial y otros abusos. En algunos casos las contraseñas, particularmente las contraseñas escritas incorrectamente, pueden aparecer en registros a pesar de que no es una práctica recomendable. La política pudiera hacer mención específica del cifrado, a pesar de no ser necesario. Si los registros se cifran, será excesivamente difícil que personas no autorizadas los puedan ver o modificar de una manera coherente. En términos de almacenamiento externo, el cifrado es la única manera verdaderamente efectiva de prevenir accesos no autorizados. Esta política requiere que un método efectivo de control de acceso esté activo.

Políticas Relacionadas: “[Desactivación, Cambio o Eliminación de Registros](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Revisión de Registros del Sistema

Política: El personal de operaciones de computación o de seguridad informática, debe revisar los registros que reflejen los acontecimientos importantes de seguridad en máquinas multiusuario de una manera periódica y a tiempo.

Comentario: Esta política requiere que el personal de operaciones de computación o de seguridad informática, revise inmediatamente los registros. Este proceso de revisión se facilita si los registros producen reportes de excepción indicando los puntos de naturaleza sospechosa que necesitan seguimiento. Sería poco práctico decirle a una persona que revise un registro que refleje todos los eventos de un sistema multiusuario muy recargado. La revisión inmediata de registros puede, por ejemplo, ser importante si hay un hacker que está intentando adivinar una contraseña a través de una línea telefónica. Si los registros no son nunca revisados, y si no hay otro mecanismo para notificar a alguien que pueda responder, la organización puede no darse cuenta de los ataques. Si los ataques no son detenidos, o por lo

menos disuadidos, diciéndole al hacker que está siendo monitoreado, el hacker se anima a continuar. Igualmente, la ventana cronológica para tomar acciones de corrección se cierra rápidamente, a menos que se inicien los pasos correctivos inmediatamente. En algunos ambientes, tales como sistemas de transferencia electrónica de fondos, la ventana en la cual los ajustes se pueden hacer es muy pequeña. En estos ambientes, el período de tiempo para revisión del registro, también puede ser incluido en la política. La política puede ser ampliada para incluir el registro de aplicaciones, en cuyo caso la gerencia de usuarios o los Propietarios de información o patrocinantes pueden involucrarse en el proceso de revisión. Debido a que filtran los registros, las herramientas como los sistemas de detección de intrusos reducen la necesidad de la revisión humana de los registros. Sin embargo, alguien debe revisar los resultados de estos sistemas y tomar medidas inmediatamente.

Políticas Relacionadas: “[Revisión de Registros de Operadores de Computadores](#)” y “[Revisión de Cambios a Registros Internos](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Monitoreo de Actividad en Internet

Política: La gerencia no debe monitorear el tráfico en Internet de un trabajador a menos que reciba una queja, en cuyo caso se habilitarán los sistemas de monitoreo existentes sin previa notificación a los trabajadores.

Comentario: Esta política informa a los trabajadores, que la gerencia es capaz de observar lo que hacen, pero que por lo general no vigila. La política es menos restrictiva que la mayoría, porque una queja puede venir de cualquier parte. Los tipos de sistemas de monitoreo, no son mencionados en esta política, con la intención de disuadir las actividades abusivas. La política enfatiza la confianza basada en el buen juicio del trabajador. La política asume una audiencia homogénea de usuarios, quienes generalmente están de acuerdo con lo que es un comportamiento moral y éticamente defendible y lo que no. Esto puede no funcionar en ambientes de trabajo muy diversos. El uso de esta política no reduce la necesidad de informar al trabajador sobre acciones específicas que no deben ser ejecutadas con los sistemas informáticos de la Empresa X.

Políticas Relacionadas: “[Registros de Uso de Internet](#)” y “[Monitoreo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

13. Herramientas de Monitoreo de Sistemas

Política: Las herramientas para el monitoreo u observación de las actividades computacionales de un usuario no se deben utilizar a menos que se notifique a los usuarios que sus trabajos serán monitoreados u observados, salvo que las herramientas se utilicen para la investigación de alguna actividad delictual.

Comentario: Los programas de monitoreo remoto pueden ser útiles para diagnosticar problemas que tengan los usuarios finales, pero también pueden ser usados para observar secretamente sus actividades en tiempo real. Existe una gran resistencia en contra de los sistemas de monitoreo que la persona desconoce. Esta política garantiza que los empleados conocen todos los sistemas de monitoreo. La política no requiere que se les informe el momento exacto en que están siendo monitoreados. Por ejemplo, un gerente puede escuchar la conversación telefónica de un vendedor con un cliente potencial a cualquier hora, siempre y cuando el vendedor haya sido notificado que ello puede suceder. La excepción involucra las investigaciones criminales, lo cual es apropiado porque la gerencia en la mayoría de los casos no quiere revelar al sospechoso que una investigación está en proceso. De hacerlo, se corre el riesgo de que el sospechoso se escape o destruya la evidencia. Algunas organizaciones pueden reemplazar las palabras "usuario de computación" por "empleado".

Políticas Relacionadas: "Recopilación Furtiva de Información Privada," "Áreas de Monitoreo Electrónico," y "Conciencia del Usuario Sobre Registros de Violaciones de Seguridad"

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

14. Notificación y Registro de Monitoreo de Usuarios

Política: Cuando una cuenta computarizada o de red de un usuario está siendo monitoreada con propósitos investigativos o disciplinarios, se debe informar inmediatamente de esta actividad al gerente del usuario involucrado, y todo el monitoreo debe ser registrado.

Comentario: Esta política garantiza que no se abusará de las herramientas de monitoreo de los trabajadores de la Empresa X, porque se requiere notificar al gerente del usuario, y también registrar la actividad. Si la política no proporciona control suficiente sobre las facilidades de

monitoreo, la Empresa X puede requerir que el gerente del usuario autorice el monitoreo secreto antes de que comience. Las organizaciones que deseen proporcionar más garantía a los usuarios, pueden requerir la notificación a la gerencia de Recursos Humanos o a un representante corporativo de ética.

Políticas Relacionadas: "Notificación de Monitoreo Electrónico del Desempeño" y "Herramientas de Monitoreo de Sistemas"

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

15. Registros de Uso de Internet

Política: Los gerentes de departamento deben recibir, revisar y aprobar los reportes de las páginas web visitadas, los archivos descargados y otros intercambios de información en Internet para las actividades de negocio del departamento.

Comentario: Esta política notifica a los usuarios que sus actividades en Internet están siendo registradas, y que un gerente de departamento determina si su uso es apropiado. La política estimula a los usuarios a seguir las políticas existentes, en especial la política referente al uso personal. La política asigna al gerente del departamento la responsabilidad de las medidas disciplinarias, no a un grupo central de seguridad informática o gerencia de Información. En realidad sólo los gerentes departamentales sabrán qué tipo de actividad es consistente con los objetivos del negocio local. Esta política es una alternativa más flexible y potencialmente más económica para el bloqueo de ciertas páginas web.

Políticas Relacionadas: "Notificación y Registro de Monitoreo de Usuarios" y "Uso Personal de Internet"

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

16. Perfiles de Uso de Internet por Clientes

Política: La Empresa X no debe captar palabras claves o pulsos del ratón o cualquier otra indicación de uso del sistema de clientes, o perfiles de uso más allá de los que se necesitan para preparar estados de facturación.

Comentario: Esta política genera confianza, lo cual conlleva a tráfico adicional en Internet. Esta política garantiza a los clientes que no se mantiene un registro de actividades y que esta información no será utilizada para comprometer su privacidad. A pesar de ser más

apropiada para los proveedores de servicios, esta política puede ser adaptada para el uso de cualquier organización que ofrezca un producto o servicio a través de Internet.

Políticas Relacionadas: “Destrucción de Registros de Transacciones,” “Información Obtenida Vía Internet,” y “Divulgación del Registro de las Actividades del Cliente”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Monitoreo del Desempeño

Política: El desempeño de los empleados de la Empresa X no se debe monitorear vía computador, a menos que el monitoreo se realice en grupos.

Comentario: El monitoreo computarizado de empleados tiene una aceptación mayor y efectiva cuando se hace por grupos, en vez de individualmente. La política no interfiere con las observaciones personales de la gerencia sobre el desempeño de empleados específicos, como la asistencia. Esta política permite el monitoreo, pero de una manera que estimula el trabajo en equipo y la aceptación del empleado.

Políticas Relacionadas: “Monitoreo o Grabación de Conversaciones Telefónicas”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

18. Actividad de Monitoreo y Grabación

Política: La información sobre las actividades de los usuarios debe ser recopilada anónimamente, a menos que se recopile con propósitos autorizados para el cumplimiento de la ley.

Comentario: Esta política permite el registro y monitoreo del sistema a la vez que garantiza la privacidad de los usuarios. La política es aplicable a páginas web, porque los usuarios se preocupan si sus actividades están siendo registradas. Estas páginas pueden incluir las que publican información sobre la que algunas personas tienen fuertes opiniones divergentes. La política especialmente incluye excepciones específicas para el cumplimiento de la ley, y puede también evitar que los hackers piensen que una política de privacidad es de alguna manera un escudo que protegerá sus actividades. La política no evita el

rastreo de los movimientos del ratón o el material que tipée un usuario específico, pero sí que se anexe la identificación de la información registrada.

Políticas Relacionadas: “Monitoreo del Desempeño” e “Información Personal para el Funcionamiento del Negocio”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Notificación de Monitoreo Electrónico del Desempeño

Política: Si corresponde, los empleados potenciales, los contratistas y consultores deben ser notificados por escrito durante su entrevista inicial de empleo que su trabajo puede ser monitoreado electrónicamente, el tipo de información que se recoge, cómo será utilizada esta información, las normas de producción existentes y las expectativas de producción para el individuo involucrado.

Comentario: Esta política evita quejas de los empleados sobre el monitoreo de desempeño, porque se les informó al respecto en la entrevista de empleo. Sin una notificación sobre los sistemas de monitoreo, los empleados pueden quejarse de que fueron mal informados de la naturaleza del empleo que ocupan. Esta política requiere que la gerencia divulgue la existencia de sistemas de monitoreo antes de que el prospecto acepte la oferta de empleo. Se pueden utilizar formularios especiales en papel firmados por los prospectos donde indiquen que fueron informados sobre los sistemas de monitoreo.

Políticas Relacionadas: “Monitoreo o Grabación de Conversaciones Telefónicas” e “Información de Empleado Potencial”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

20. Monitoreo de Mensajes de Correo Electrónico

Política: Los mensajes enviados por el sistema interno de correo electrónico de la Empresa X pueden ser leídos por la gerencia y administradores de sistemas de la Empresa X.

Comentario: Esta política aclara que la gerencia y el personal técnico pueden leer los mensajes de correo electrónico de los empleados. Esto es una política de “puede” en vez de “debe”. Para evitar problemas legales,

una organización que monitorea el correo electrónico debe efectuar todos los esfuerzos posibles para informar a sus empleados que se está haciendo un monitoreo. Si se les notifica de antemano, los empleados pueden cambiar su patrón de uso para reflejar el hecho de que pueden ser monitoreados. Este cambio resultante en comportamiento es totalmente consistente con una política que indica que los sistemas de la organización deben ser utilizados solamente para propósitos de negocio.

Políticas Relacionadas:“Uso Distinto al Empresarial de la Información de la Organización,” “Examen de los Datos Almacenados en los Sistemas,” “Monitoreo de Mensajes de Correo Electrónico,” y “Privacidad en Correo Electrónico”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

21. Registro de Inhabilitaciones

Política: Cada vez que los controles de sistemas sean inhabilitados, se debe generar un registro, el cual debe ser prontamente revisado respecto de los cambios efectuados y los comandos privilegiados que se utilizaron.

Comentario:Esta política especifica cuándo se deben generar y revisar los registros de inhabilitación de los controles y qué debe determinar la gerencia al revisar los registros. La utilización de reportes de excepción reduce el tiempo que toma la revisión. Si no existe un registro que refleje el uso de las funciones de inhabilitación de los controles, los usuarios privilegiados estarían tentados a abusar de estas funciones. En algunos casos los sistemas de detección de intrusos pueden efectuar automáticamente esta revisión de registros.

Políticas Relacionadas:“Facilidades para Inhabilitar Controles” y “Uso de la Inhabilitación de los Controles”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

22. Información Obtenida Vía Internet

Política: Cada vez que la Empresa X recopile información sobre las personas que visitan su pagina web, debe notificar a los usuarios sobre este proceso de monitoreo, darles la oportunidad de especificar cómo va a ser utilizada esa información y notificarles a quién se divulgará la información.

Comentario:Las páginas web tienen la habilidad de recolectar muchos tipos de información sobre los individuos que las han visitado. La información que está disponible incluye las pantallas que han examinado, por cuanto tiempo y dónde pulsaron el cursor. Las direcciones de correo electrónico de Internet también se pueden recolectar sin el conocimiento del usuario. Hay herramientas disponibles que permiten al usuario ver cuáles mensajes ha colocado un individuo en Usenet. Con las ansias de los trabajadores de mercadeo de obtener un retrato definitivo de las actividades de las páginas web de Internet, hay una presión considerable para utilizar estos nuevos datos disponibles. Esta política evita una reacción violenta y repentina de los grupos pro-privacidad, lo que puede conducir a una mala publicidad para la organización que estableció o que es propietaria de la página web.

Políticas Relacionadas:“Privacidad de la Información del Cliente” y “Opción de Participación en Sistema de Datos Privados”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

9.07.03 Sincronización del Reloj

1. Sincronización del Reloj

Política: Todos los computadores multiusuario conectados a la red interna de la Empresa X deben siempre tener la hora actual reflejada en sus relojes internos.

Comentario:El tener los relojes sincronizados ayuda al diagnóstico de los problemas del sistema y su solución, principalmente en los sistemas cliente-servidor y otros sistemas que involucren hardware interdependiente.

Esta política también ayudará a tener registros confiables de los eventos, actualizaciones automáticas de software, duplicación de bases de datos, cambios automáticos de claves de cifrado y otras actividades relacionadas con seguridad. Esta política permite a los investigadores rastrear con confianza las acciones de los hackers u otros intrusos no autorizados de la red. Si los relojes no están sincronizados y no son precisos, entonces las investigaciones pueden verse obstaculizadas. La evidencia descubierta seguramente no será

confiable, y por ende inútil como la razón para una acción disciplinaria o un juicio. Los relojes internos precisos son aún más importantes porque algunos controles de acceso dependen de esta información, como los mecanismos que permiten a los usuarios utilizar comandos privilegiados sólo durante las horas de trabajo. Todos los relojes deben estar fijados a la hora local, y deben ser inmediatamente cambiados para reflejar los cambios periódicos que se hacen durante el año. Cuando ocurra una caída del sistema, una falla de electricidad, una actualización del sistema operativo, o cualquier otro evento que puede haber afectado al reloj,

el reloj debe ser actualizado rápidamente. Los relojes de los computadores varían a medida que pasa el tiempo, y por ello deben ser periódicamente sincronizados. La política puede ser ampliada a todos los sistemas computarizados conectados a la red pero es más importante para los sistemas multiusuario.

Políticas Relacionadas: “[Desactivación, Cambio o Eliminación de Registros](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9.08 Computación Móvil

9.08.01 Computación Móvil

1. Uso de Pequeños Computadores Portátiles

Política: Los asistentes digitales personales, los computadores portátiles y los teléfonos inteligentes no se deben utilizar para información de negocios de la Empresa X, a menos que hayan sido configurados con los controles necesarios y autorizados para dicho uso por la gerencia de Seguridad Informática.

Comentario: Los dispositivos incluidos en esta política son convenientes y útiles, pero pueden exponer la información de la Empresa X a divulgación no autorizada. Los usuarios pueden optar por la facilidad en lugar de la seguridad y esta política evita esa decisión. La política reconoce que estos dispositivos frecuentemente carecen de medidas de seguridad adecuadas. La mayoría de estos y otros sistemas pequeños han sido utilizados simplemente como calendarios y libretas de direcciones sofisticadas. Pero el extenso uso de las capacidades inalámbricas disponibles, cambiarán radicalmente la forma en que se utilizan estos pequeños computadores. Las comunicaciones cifradas para estas transmisiones inalámbricas están disponibles, pero muchos usuarios prefieren no usar esta característica. Esta política garantiza que estos nuevos dispositivos son adecuadamente seguros para utilizarlos en la información del negocio. Si bien un empleador puede no tener jurisdicción sobre la propiedad personal de un individuo, sí tiene el derecho de imponer límites a su propia información.

Políticas Relacionadas: “[Teléfonos Celulares o Inalámbricos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

2. Información Sensible en Pequeños Computadores

Política: Los mecanismos de seguridad disponibles en los asistentes digitales personales, computadores portátiles, teléfonos inteligentes y similares, no deben ser utilizados con información sensible de la Empresa X.

Comentario: Esta política prohíbe el uso de computadores pequeños portátiles con información sensible de la Empresa X para evitar la divulgación no autorizada de esta información. Esto podría pasar simplemente con el robo o pérdida de uno de estos dispositivos o porque un usuario no sabe cómo operar debidamente los mecanismos de seguridad disponibles en estos computadores pequeños. La política asume que el término “información sensible” ha sido definido a través de un esquema de clasificación de datos. Si éste no fuese el caso, entonces la política puede ser modificada para prohibir que se maneje información de la Empresa X en estos pequeños computadores, a pesar de que esto puede degradar adversamente la productividad del trabajador.

Políticas Relacionadas: “[Protección de la Reinicialización Basada en Contraseña](#),” “[Información Secreta en Computadores Portátiles](#),” y “[Préstamo de Computadores Que Contienen Información Sensible](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

3. Información Secreta en Computadores Portátiles

Política: Los empleados que posean dispositivos portátiles, un laptop, un libro de anotaciones, agenda u otro dispositivo similar que contenga información confidencial de la Empresa X, no deben dejarlos desatendidos a menos que la información esté cifrada.

Comentario: Esta política evita que la información secreta caiga en manos de personas no autorizadas. Robar los computadores portátiles personales de los ejecutivos se ha convertido en una técnica normalizada de espionaje industrial. El cifrado de los datos contenidos en el disco duro es la única forma definitiva de evitar la divulgación que conllevaría dicho robo. Idealmente, todo lo contenido en el disco duro debe estar cifrado y el usuario debe proporcionar una contraseña para poder tener acceso a los datos. Una cantidad de productos de bajo costo en el mercado apoyan esta política. El gran número de computadores muy pequeños disponibles hace que esta política sea apropiada. Sin embargo, para los sistemas muy pequeños como agendas de bolsillo puede no haber disponibilidad de sistemas comerciales de cifrado. Mientras dichos productos no estén disponibles, será necesario mantener fuera de estos sistemas la información secreta. La palabra "secreta" en la política puede ser reemplazada por "sensible" o por un conjunto de términos de clasificación de datos usado por la organización. Esta política asume que el término "secreto" ya ha sido definido.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Remoción de Información Sensible en Papel,” “Computadores Portátiles en Aviones,” y “Cifrado en Medios de Respaldo”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

4. Uso de Computadores Portátiles

Política: Hasta tanto se emitan los requerimientos para la operación segura de computadores portátiles, los trabajadores no deben utilizar estos sistemas para procesar información de la Empresa X clasificada como confidencial o secreta.

Comentario: Esta política emite de inmediato una política a pesar de que la organización no haya tenido tiempo de ejecutar una evaluación de riesgo o considerar seriamente lo que debe hacer respecto de la computación móvil, teletrabajadores y asuntos relacio-

nados con la seguridad. Esta política asume que se ha adoptado un sistema de clasificación de datos. Si éste no es el caso, la política puede ser modificada para prohibir el uso de estas máquinas con datos de la Empresa X que no hayan sido públicamente divulgados. Se pueden hacer excepciones para libretas de direcciones, listas de números de teléfono y libretas de programación contenidas en estas máquinas. La política es importante porque es una manera inmediata de controlar la utilización de estas máquinas. Después de que la gerencia haya aclarado los requerimientos para la seguridad de sistemas portátiles, esta política podrá ser reemplazada con instrucciones más específicas de seguridad.

Políticas Relacionadas: “Información Sensible en Pequeños Computadores” y “Uso de Pequeños Computadores Portátiles”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

5. Computadores Portátiles con Información Sensible

Política: Todos los computadores portátiles, laptops, libretas y otros computadores transportables que contengan información sensible de la Empresa X, deben emplear consistentemente el cifrado en el disco duro para todos los archivos y protección de arranque en el funcionamiento del computador.

Comentario: Esta política protege la información sensible almacenada en los computadores portátiles. Esta máquinas son frecuentemente robadas, extraviadas o simplemente desaparecen. Desafortunadamente, cuando esto pasa, la información almacenada en las unidades de discos duros de esas máquinas se pierde. A pesar de que el costo de los paquetes de hardware y software es significativo, es mucho menor que el costo de la información almacenada. El único método confiable para proteger esta información si las máquinas están desatendidas es el de cifrar la información en la unidad del disco duro. Esta política requiere que todos los archivos almacenados en el disco duro se cifren. El cifrado en segundo plano de todos los archivos hace del proceso de cifrar y descifrar una función del sistema en vez de algo que el usuario debe invocar. Este procedimiento también impone una penalidad en el desempeño. Esta política va más allá, al requerir que se proporcione una contraseña en el momento en que la máquina se activa. En muchos casos los dos controles mencionados en esta política necesitarán ser adquiridos como sistemas separados de hardware o software.

Políticas Relacionadas:“[Información Secreta en Computadores Portátiles](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

6. Computadores Portátiles en Aviones

Política: Los empleados que viajen en avión con computadores portátiles, laptops, ordenadores portátiles y otros similares que contengan información sensible de la Empresa X, no deben enviarlos por el sistema de equipaje de la línea aérea.

Comentario:Esta política evita el robo o pérdida de computadores portátiles que contengan información sensible. Los robos en los equipajes de las líneas aéreas hacen peligroso el registrar un computador como equipaje aunque esté dentro del equipaje. Muchas piezas de equipaje son enviadas a direcciones incorrectas o se pierden después de recibir las líneas aéreas. Conservar la máquina en posesión del usuario es un procedimiento menos riesgoso. Esta política no es necesaria si toda la información del usuario en el disco duro del computador y en los medios de almacenamiento que la acompañan está cifrada. Pero aunque la información esté cifrada, el impacto financiero del reemplazo del hardware podría ser significativo. Algunas organizaciones podrían incrementar la política para permitir una excepción a este procedimiento cuando sean utilizados los procesos de cifrado.

Políticas Relacionadas:“[Información Secreta en Computadores Portátiles](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

7. Información Sensible en Computadores Personales

Política: Si se almacena información sensible en el disco duro o en otros componentes internos de un computador personal, la información se debe proteger mediante una contraseña de control de acceso o cifrándola.

Comentario:Esta política está dirigida a delinear procedimientos especiales para el manejo de información sensible en computadores personales (PC). Debido a que los PC no siempre son seguros, personas no autorizadas pueden tener acceso físico a ellos, y por ende a la información sensible. Esta política asume que el término "sensible" ha sido previamente definido en

otro documento relacionado a las políticas. El término "sensible" puede ser cambiado a "confidencial" o a palabras similares. Las palabras "u otros componentes internos" se utilizan para reconocer que la memoria flash no volátil y otros subsistemas de memoria internos del PC pueden contener información sensible, aunque hablando con propiedad, no son un disco duro interno. Esta política es importante para los computadores portátiles y manuales, laptops, y otras máquinas transportables, no sólo para las máquinas de escritorio. Las organizaciones pueden también estudiar la posibilidad de utilizar etiquetas para discos especiales y otros medios de almacenamiento como los que incorporan códigos de barras.

Políticas Relacionadas:“[Etiquetado Durante el Ciclo de Vida de la Información](#),” “[Etiquetado Completo de la Clasificación](#),” y “[Almacenamiento de Información Sensible](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

8. Préstamo de Computadores Que Contienen Información Sensible

Política: No se debe prestar a nadie un computador personal, un computador manual, un computador transportable, un asistente personal digital, un teléfono inteligente o cualquier otro computador utilizado para actividades de negocios que contenga información sensible.

Comentario:Esta política prohíbe a los empleados que prestan su máquina personal a otros. Una variedad de controles, como los controles de inicio basados en contraseñas fijas para computadores personales y medidas de cifrado se establecen para un individuo específico, tomando en cuenta las tareas propias de su puesto actual y su necesidad de conocer. El permitir que otra persona tenga acceso a esa máquina es permitir que esa otra persona evite los controles. El permitir que otros usen un computador personal también perjudicaría la veracidad de los registros y de otros mecanismos que monitorean el comportamiento del usuario. Los computadores personales necesitan ser considerados como únicos y específicamente asignados a cierto individuo, al igual que la identificación personal del usuario. La palabra "sensible" tendrá que ser definida en otra parte.

Políticas Relacionadas:“[Identificador Único de Usuario y Contraseña Obligatorios](#)” y “[Contraseñas Compartidas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

9. Propiedad de la Organización en Sitios Alternativos de Trabajo

Política: Deben tomarse precauciones razonables en los sitios alternativos de trabajo, para proteger el hardware, el software y la información de la Empresa X de robo, daño y abuso.

Comentario: Esta política notifica a los teletrabajadores y otros que trabajan con los sistemas informáticos de la Empresa X en ubicaciones diferentes a la sede central, que las mismas medidas de seguridad se aplican sin importar donde estén ubicados. La información debe ser protegida de manera consistente por su valor, sensibilidad y criticidad. Las medidas de protección deben aplicarse sin importar la ubicación de la información, la forma que adquiera y la tecnología utilizada para manejarla. Por ejemplo, si se está manejando información sensible, éstase debe cifrar cuando se almacene, no importa si el computador está en la oficina principal o en un sitio alternativo. Esta política permite a la organización evitar tener que especificar un conjunto nuevo de requerimientos de control para el manejo externo de la información.

Políticas Relacionadas: “Protección de la Información,” “Remoción de Información Sensible,” y “Descarga de Información Sensible”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

10. Información Almacenada en Computadores Portátiles Propiedad de la Organización

Política: La información almacenada en computadores portátiles de la Empresa X es propiedad de ella y la Empresa X la puede inspeccionar o utilizar de cualquier manera y a cualquier hora y, al igual que el equipo, debe ser devuelta a la Empresa X al momento en que el empleado cese su relación laboral con la Empresa X.

Comentario: Esta política impide confusiones acerca de la propiedad de la información almacenada en los computadores portátiles. Debido a que viajan con ellos, algunos empleados los consideran propiedad personal. Esta política aclara esa perspectiva al declarar en la política que estos dispositivos se entregan para ejecutar tareas específicas y que deben usarse sólo para

propósitos de negocios. Después de leer esta política los usuarios de estos dispositivos saben que no deben almacenar información privada ya que un auditor de la Empresa X puede examinar su contenido en cualquier momento. Esta política extiende los límites entre la propiedad organizacional y la propiedad personal del empleado, ya que la tecnología permite nuevos tipos de computación distribuida. Suponiendo que no se emitió ninguna política sobre este tema, si un empleado utiliza su equipo propio, entonces el empleador no tiene derecho sobre la información allí contenida.

Políticas Relacionadas: “Información Sensible en Computadores Personales” y “Retención de Información al Terminar Empleo”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Posesión de los Computadores Portátiles

Política: Los empleados deben mantener los computadores portátiles de la Empresa X en su poder todo el tiempo, a menos que los hayan depositado en un lugar seguro, como por ejemplo en un armario cerrado con llave o en la caja fuerte de un hotel.

Comentario: Esta política limita la pérdida de computadores portátiles por robo y la pérdida de información almacenada en dichos computadores. En la medida que un computador esté en poder del empleado, existe menos posibilidad de que sea robado. Si se deja en una oficina desatendida o en un lugar relativamente público, lo más probable es que el usuario no lo consiga a su regreso. Esta política no dice nada sobre sistemas de cifrado o sistemas de control de acceso, importantes para computadores portátiles, pero que pueden ser considerados en otras políticas.

Políticas Relacionadas: “Computadores Portátiles con Información Sensible,” “Información Secreta en Computadores Portátiles,” y “Tarjetas de Contraseñas Dinámicas”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Alternativas para Computadores Móviles

Política: Cuando estén fuera de las oficinas de la Empresa X, los usuarios de computadores móviles deben utilizar un software de cifrado para proteger la

información sensible almacenada, o emplear alguna técnica para asegurar físicamente el medio que contiene la información sensible.

Comentario: Esta política especifica cómo los usuarios de computadores móviles deben proteger la información sensible de la Empresa X cuando se encuentran lejos de las oficinas. La política especifica alternativas que involucran el ocultar la información sin removerla de la máquina o proteger físicamente la información. Es necesaria una atención especial para los computadores móviles, porque son los más susceptibles al robo. Con esta política, el robo del computador cuando no está en poder del empleado, no resultará en la divulgación no

autorizada de información sensible. Esta política asume que el empleado conoce lo que es sensible y qué no lo es. Si esta distinción no se ha hecho, la organización puede requerir al menos uno de estos enfoques para toda la información de la Empresa X contenida en un computador móvil.

Políticas Relacionadas: ‘Equipo de Teletrabajo,’ ‘Viajes con Información Secreta,’ y ‘Exposición Pública de Información Sensible’

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

9.08.02 Teletrabajo

1. Operadores de Entrada de Datos

Política: Todos los operadores de la Empresa X que realicen el trabajo de introducción de datos deben emplear clientes simples, tal como los configure la gerencia de Sistemas Informáticos y descargar el software para su trabajo al comienzo de cada día de trabajo.

Comentario: Esta política refleja un ambiente de alta seguridad en donde los operadores que dan entrada a los datos utilizan sus máquinas sólo para actividades de negocios de la Empresa X. Debido a que las máquinas son clientes simples, no tienen disco duro y no pueden permanentemente almacenar el software que ejecutan. Con este enfoque, cada transacción que se completa se debe enviar a un servidor de la Empresa X, que es en donde se almacenan todos los datos del negocio. Si los dispositivos de la periferia como la unidad de disquete están bloqueados, este enfoque evita que el teletrabajador tome electrónicamente información que es propiedad de la Empresa X. La configuración debe tener un modem rápido u otro tipo de conexión porque el software es bastante grande, y puede tomar algún tiempo descargarlo. También, esta configuración asume que está disponible una conexión relativamente confiable a la red. De otra forma, el trabajo del teletrabajador se verá afectado cuando ocurran interrupciones de comunicación. Este enfoque es restrictivo, y no es apropiado para los teletrabajadores de la oficina. Este enfoque permite que la Empresa X cambie diariamente el software si fuese necesario y para garantizar que todas las máquinas de los clientes serán actualizadas al mismo tiempo. Se puede utilizar un mecanismo de control de cambios en los clientes simples para evitar cambios en los sistemas operativos u otro software.

Políticas Relacionadas: ‘Estaciones de Trabajo Sin Discos,’ ‘Descarga de Software,’ y ‘Descarga de Información Sensible’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Equipo de Teletrabajo

Política: Los empleados de la Empresa X que trabajen en sitios alternativos deben utilizar computadores y equipos de redes proporcionados por la Empresa X, a menos que el Centro de Atención al Usuario autorice el uso de otro equipo compatible con los sistemas y controles informáticos de la Empresa X.

Comentario: Esta política garantiza que los teletrabajadores no utilizarán sistemas informáticos que puedan causar un mal funcionamiento o daño a los sistemas o a la información de la Empresa X, o no proporcionen protección suficiente a la información de la Empresa X. Esto último por ejemplo, puede ocurrir si el equipo de teletrabajo no es capaz de cifrar la información almacenada en un computador en la casa de un empleado. Un robo podría entonces causar la divulgación no autorizada de esta información sensible. Muchas organizaciones tienen una lista del equipo normal de sistemas informáticos entregado a los teletrabajadores. Esta lista puede incluir un modem, una línea telefónica de alta velocidad, buscadoras, máquina contestadora, un fax, una copiadora, una impresora y un computador personal. La lista podría incluir software y documentación como programas normales de aplicaciones y funciones normales. Las organizaciones podrían publicar una política separada que establezca

que la Empresa X no es responsable por pérdidas, daños o uso y desgaste de un equipo propiedad del empleado utilizado para negocios de la Empresa X. También sería deseable mencionar que el equipo propiedad del empleado se puede continuar utilizando para actividades personales siempre y cuando no se comprometa la información de la Empresa X. Estas políticas se deben complementar con palabras que definen lo términos como "sitio alternativo de trabajo" y "teletrabajo".

Políticas Relacionadas: "Requisitos de Seguridad para Teletrabajo," "Computadores Portátiles con Información Sensible," y "Gabinetes Metálicos con Cerradura"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

3. Ambientes de Teletrabajo

Política: Para retener el privilegio de trabajar externamente, todos los teletrabajadores deben estructurar su ambiente de trabajo remoto para que esté de acuerdo con las políticas y normas de la Empresa X.

Comentario: Esta política tiene la intención de informar a los teletrabajadores que ser un teletrabajador es un privilegio, no un derecho, y como tal este privilegio puede revocarse si los trabajadores no cumplen las políticas y normas de la Empresa X. La política claramente evita dictar las especificaciones de los ambientes remotos de trabajo, porque pueden cambiar. Las especificaciones de seguridad incluyen el mantener los equipos y otros materiales en un salón cerrado, y el uso regular de un protector de ondas erráticas, un sistema de control de acceso basado en contraseñas para el disco duro, una máquina trituradora de papeles y un programa de protección contra virus. Existen otras especificaciones no relacionadas a seguridad que tratan los temas de recursos humanos, como responsabilizarse por el tiempo trabajado.

Políticas Relacionadas: "Reautorización de los Privilegios de Acceso de Usuario" e "Información Secreta en Computadores Portátiles"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Requisitos de Seguridad para Teletrabajo

Política: Antes de que pueda comenzar un convenio de teletrabajo, el gerente del trabajador debe estar satisfecho de que el sitio alternativo de trabajo es apropiado para que el trabajador ejecute trabajos para la Empresa X.

Comentario: En los últimos años se han hecho más frecuentes las discusiones sobre sitios alternativos de trabajo. Cada vez que se estudian estos convenios, es importante considerar lo que sucede con los activos físicos e informáticos de la Empresa X. Esta política tiene la intención de dar a la gerencia una amplia latitud para decidir a quién se permitirá teletrabajar, y bajo qué circunstancias. Muchas organizaciones han adoptado un listado con los requerimientos de seguridad para los teletrabajadores. Estos generalmente incluyen herramientas como paquetes de cifrado de discos duros, archivos con llave y máquinas trituradoras de papel. Algunas organizaciones exigen que los teletrabajadores firmen una declaración donde prometen cumplir las reglas específicas para proteger la información remota. La política puede ser aumentada con términos que aclaren las definiciones de "sitio alternativo de trabajo" y "teletrabajadores".

Políticas Relacionadas: "Pases de Propiedad," "Software Antivirus Actual," y "Gabinetes Metálicos con Cerradura"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Procedimientos de Seguridad Informática en Teletrabajo

Política: Los teletrabajadores deben cumplir todas las políticas de seguridad de los sistemas remotos incluyendo, sin limitantes, el cumplimiento de los convenios de licencia del software, ejecución de respaldos regulares y el uso de máquinas trituradoras de papel para disponer de la información sensible impresa.

Comentario: Esta política pone en conocimiento de los teletrabajadores los procedimientos que deben seguir día a día. Algunas organizaciones necesitarán una descripción más detallada de los requerimientos de seguridad asociados al teletrabajo, en cuyo caso la política puede ser ampliada a través de una nota aparte. Las organizaciones querrán aumentar esta lista de precauciones con otras consideraciones, como la devolución del equipo de la organización en el momento en que la relación de trabajo termine. Si una organización va a permitir que su información sensible se utilice

en sitios remotos que no pueden ser fácilmente supervisados, es razonable que insista en que se observen las precauciones de seguridad. Debido a que el teletrabajo introduce nuevos riesgos, es apropiada una política estricta y documentada sobre los teletrabajadores en los casos donde no existe una política similar para los trabajadores que vienen todos los días a trabajar en la oficina. Esta política es apropiada para trabajadores que no son teletrabajadores, pero que sin embargo, se llevan información de la organización a sus casas o en viajes de negocio.

Políticas Relacionadas: “Convenios con Terceros” y “Convenio de Cumplimiento”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Inspección de Ambientes de Teletrabajo

Política: La Empresa X debe mantener el derecho a conducir inspecciones de las oficinas de los teletrabajadores con previo aviso de sólo uno o más días.

Comentario: Esta política informa a los teletrabajadores que los representantes de la Empresa X pueden conducir inspecciones en sus oficinas. Esto garantizará que los teletrabajadores cumplan las políticas y procedimientos de seguridad y protección. Otorgando a los empleados el permiso para teletrabajar, la Empresa X recibe el derecho de conducir inspecciones de su propiedad que se encuentre en las casas de los teletrabajadores. Mediante la conducción de inspecciones, la gerencia de la Empresa X está cumpliendo con su deber de proteger los activos de la Empresa. No es necesaria una política separada para notificar a los usuarios del computador que el auditor examinará los controles en las oficinas de la organización y, ya que sus casas son el dominio del empleado, el derecho a inspeccionarlas se debe comunicar y negociar claramente. Una inspección se conduce normalmente tan pronto como el trabajador ha establecido su oficina. En adelante, inspecciones anuales o solicitadas son suficientes. La política permite múltiples inspecciones de seguimiento para corregir deficiencias que se hayan encontrado en visitas anteriores. Algunas organizaciones no querrán dar aviso previo.

Políticas Relacionadas: “Revisión de los Controles de los Sistemas Informáticos — Interno”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Gabinetes Metálicos con Cerradura

Política: Todos los trabajadores que deban mantener información confidencial de la Empresa X para realizar su trabajo en sus casas, deben recibir mobiliario de metal con cerradura para el almacenamiento adecuado de esta información.

Comentario: Esta política garantiza que los teletrabajadores y otro personal que trabajan en sus casas tengan el mobiliario adecuado para almacenar la información sensible de la Empresa X con seguridad. Si un trabajador ya tiene el mobiliario adecuado, la Empresa X no tendrá la necesidad de proporcionárselo y si el mobiliario se le proporcionó, la propiedad de éste la conserva la Empresa X. Las etiquetas en los muebles deben demostrar esto, y una nota al empleado aclarando la propiedad también es recomendable. Para hacer esta política más selectiva, la palabra "sensible" se puede remplazar por la palabra "secreta". Esta política asume que la palabra "sensible" ha sido definida en otra parte. Con el aumento del número de personas que trabajan en sus carros o camionetas, esta política podría ser ampliada para incluir vehículos de transporte. La política también puede ser ampliada para incluir otras herramientas para el trabajo en casa, tales como programas de cifrado para un computador personal o estación de trabajo.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Equipo de Teletrabajo,” “Seguridad de la Información Sensible,” “Requisitos de Seguridad para Teletrabajo,” y “Remoción de Información Sensible”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

10 DESARROLLO Y MANTENIMIENTO DE SISTEMAS

10.01 Requerimientos de Seguridad de los Sistemas

10.01.01 Análisis y Especificaciones de los Requerimientos de Seguridad

1. Identificación de Requisitos de Seguridad

Política: Antes de desarrollar o adquirir un nuevo sistema, la gerencia del departamento usuario debe haber especificado claramente los requisitos relevantes de seguridad.

Comentario: Esta política requiere que el gerente del departamento usuario considere los requisitos de seguridad en una fase temprana del ciclo de vida de desarrollo de los sistemas (SDLC, por sus siglas en inglés). Si existe un SDLC formal, entonces la política podría extenderse para hacer referencia a señales específicas en el proceso en donde debería existir una consideración de seguridad. Esta política establece claramente que el gerente del departamento usuario o tal vez el Propietario de la información son los responsables de incorporar controles pertinentes en un nuevo sistema. El gerente involucrado puede y debe solicitar asistencia de consultoría del gerente de Seguridad Informática. El ámbito de esta política puede expandirse para incluir a los sistemas significativamente modificados y no únicamente a los nuevos sistemas. Deberá definirse qué constituye una actualización o cambio significativo.

Políticas Relacionadas: “[Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas](#)” y “[Especificaciones para Software Desarrollado Internamente](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

2. Propuestas para Desarrollar Sistemas Internos

Política: Toda propuesta de proyecto de desarrollo interno de sistemas informáticos con un presupuesto propuesto por encima de \$ 100.000 debe ser copiada a la gerencia de Seguridad Informática al mismo tiempo que se distribuya a la alta gerencia para su revisión y aprobación.

Comentario: Esta política garantiza que la gerencia de Seguridad Informática será incluida en la discusión cuando la gerencia considera el desarrollo de grandes proyectos. En algunas organizaciones, la gerencia de

Seguridad Informática es tomada en cuenta únicamente cuando el proyecto se ha completado o antes de ir a producción. Estudios independientes indican que es 10 veces más costoso añadir controles a una aplicación de negocios después de que vaya a producción en lugar de antes. Esta política asegura que la gerencia de Seguridad Informática esté involucrada en todo proyecto grande relacionado con los sistemas informáticos. Una propuesta también identificará los miembros del personal de la gerencia que están involucrados, de forma tal que la gerencia de Seguridad Informática puede contactar directamente a esas personas cuando lo necesite. No existe nada en especial acerca de la cantidad monetaria mencionada en la política. Esta podría fácilmente haber sido otra figura.

Políticas Relacionadas: “[Evaluación de Nuevas Tecnologías](#)” y “[Enunciados Sobre el Impacto de la Seguridad](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Inclusión de Seguridad en Sistemas

Política: Los desarrolladores de sistemas internos deben incrustar la seguridad dentro de los sistemas que construyan o mejorar todas las instancias en las que haya una solución disponible comercialmente, a costo razonable y generalmente aceptada.

Comentario: Esta política ahorra dinero y hace que los sistemas sean más fáciles de usar. Los estudios demuestran que las organizaciones que añaden controles después de que una aplicación de negocios va a producción, pagarán 10 veces más que aquellas organizaciones que integran la seguridad durante el proceso de desarrollo. Esta política requerirá un mayor gasto por adelantado, pero reducirá el costo de la seguridad informática a largo plazo. Utilizar paquetes de seguridad informática provistos por terceros reduce los costos a largo plazo. Siempre que sea posible, la seguridad informática debe ser automatizada y removida del dominio del usuario. Por ejemplo, a los usuarios no se les pedirá que respalden sus datos residentes en un computador de escritorio. En lugar de esto, puede

emplearse un proceso automático de respaldo a un servidor en una red de área local. Esta política pretende eliminar la seguridad del dominio del gerente del departamento usuario. Esta política asume que no se ha publicado y endosado ninguna arquitectura de seguridad por la gerencia. Si esta arquitectura existe, los desarrolladores deben suscribirse a los requisitos que en ella se encuentren.

Políticas Relacionadas: “Facilidad de Uso de los Controles de Seguridad” e “Identificación de Requisitos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Especificaciones para Software Desarrollado Internamente

Política: Todo software desarrollado por personal interno que se utilice para procesar información sensible, valiosa o crítica debe poseer una especificación formal por escrito que forme parte de un acuerdo entre el Propietario de la información y el desarrollador del sistema, redactada y elaborada antes de que comiencen los esfuerzos de programación.

Comentario: Las especificaciones formales definen la funcionalidad sobre la cual pueden depender los usuarios, desarrolladores, auditores y terceros. Las especificaciones formales deben también especificar claramente las medidas de control que deben ser incorporadas al software. Esta política tiene como objetivo asegurar que el Propietario de la información ha especificado lo que se entregará antes de que empiecen los esfuerzos de programación. Esta política está deliberadamente dirigida a enfrentar el problema que se presenta cuando los desarrolladores comienzan a trabajar antes de que se clarifique la naturaleza del sistema en cuestión. Nada en esta política evita el uso de prototipos como un mecanismo para refinar los requisitos, para probar nuevas ideas o para solicitar consideraciones del usuario. Una especificación puede ser modificada a medida que avanza el trabajo, a medida que los usuarios entienden mejor lo que necesitan y cuando los requisitos del negocio cambian. Esta política únicamente requiere una especificación previa. Algunas organizaciones pueden desear ser más específicas acerca de lo que debe colocarse en la especificación. En la mayoría de los casos, lo que se colocará en una especificación aceptable se definirá en otro lugar, como dentro

de la documentación del desarrollo de sistemas. Debido a que la especificación tiene que ver con información que es del interés de la gerencia de Seguridad Informática, algunas organizaciones desearán añadir la aprobación del gerente de Seguridad Informática a la aprobación del Propietario de la información. Esta política es particularmente relevante para aquellos ambientes en los que los usuarios finales hacen su propia programación, como los ambientes cliente-servidor, intranets, redes de área local y computadores personales, debido a que estos nuevos programadores pueden no estar familiarizados con los enfoques tradicionales de desarrollo de sistemas.

Políticas Relacionadas: “Análisis del Impacto sobre la Seguridad Informática”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Principios de Codificación de Aplicación

Política: Deben utilizarse principios y prácticas seguras de codificación, especificados y actualizados por la gerencia de Seguridad Informática para todo el software desarrollado o mantenido internamente.

Comentario: Esta política garantiza que los desarrolladores observarán los principios y prácticas seguras de codificación cuando escriben el código de computación. Un resumen de las vulnerabilidades históricas indica que los mismos problemas de programación ocurren en repetidas ocasiones. Por ejemplo, el desbordamiento de los buffers es fácil de prevenir, pero cuando los programadores no se protegen adecuadamente, la seguridad puede y a menudo se ve comprometida. Estos principios y prácticas de codificación segura circundan una variedad de consideraciones que deben ser integradas dentro del ciclo de vida del desarrollo de sistemas. Estas consideraciones incluyen la evaluación de riesgo, documentación y prueba. Una excepción a esta política puede ser provista por las macros incrustadas en hojas de cálculo, en documentos de procesadores de palabras y en bases de datos mantenidas por el usuario.

Políticas Relacionadas: “Especificaciones para Software Desarrollado Internamente” e “Identificación de Requisitos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Herramientas y Técnicas de Desarrollo Maduras

Política: Todos los proyectos de desarrollo interno de software deben utilizar herramientas y técnicas de desarrollo maduras.

Comentario: La utilización de herramientas y técnicas nuevas o no probadas como los compiladores nuevos, aumenta los riesgos asociados con el desarrollo de proyectos y los resultados obtenidos. Por ejemplo, los desarrolladores pueden no estar prevenidos acerca de los problemas de seguridad con nuevas herramientas o técnicas y pueden permitir inadvertidamente que los resultados de estos problemas sean incorporados a los sistemas de producción. Las herramientas y técnicas maduras por lo general han corregido las imperfecciones y los problemas, mientras que por el contrario, las herramientas y técnicas nuevas no lo han hecho. Las herramientas maduras son ofrecidas por lo general por proveedores que han estado en el negocio un largo lapso y muy probablemente son financieramente estables. Esta política elimina los problemas que podrían traer las nuevas herramientas y técnicas. Esta política también involucra un intercambio. Por motivos competitivos y otras razones, la gerencia puede querer utilizar nuevas herramientas y técnicas. Debido a que en la política no se especifica la definición de madura, existe alguna amplitud para que la gerencia investigue nuevas herramientas y técnicas, cuando éstas parezcan poder realizar el trabajo que la gerencia quiere; y si han recibido buenas críticas en los medios o de otros clientes, pueden declararlas maduras.

Políticas Relacionadas: “[Versiones de Sistemas Operativos](#)” e “[Interfaces a Redes Externas](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

7. Lenguajes de Programación de Alto Nivel

Política: Todos los proyectos de desarrollo interno de sistemas que involucren un esfuerzo de más de \$100.000 deben ser programados en un lenguaje aprobado de más alto nivel, a menos que se obtenga permiso de la gerencia de Sistemas Informáticos.

Comentario: Esta política asegura que el equipo desarrollador utilice en forma consistente lenguajes de alto nivel. La organización puede especificar en la política cuáles lenguajes son permitidos. Esto es importante cuando los usuarios finales hacen su propia programación fuera del alcance de Sistemas

Informáticos. Al limitar la naturaleza y clases de lenguajes permitidos, esta política asegura la capacidad de mantenimiento y control de los esfuerzos de programación de los usuarios finales, particularmente en los ambientes cliente-servidor, de redes de área local, intranets y computadores personales. Los módulos para procedimientos de seguridad como el cifrado serían objetos predefinidos, que podrían ser incorporados en las aplicaciones de negocios a través de un ambiente de programación orientado a objetos. Los Sistemas Informáticos deben fijar la norma para los lenguajes de más alto nivel a emplearse y deben manejar las excepciones. No existe nada en especial acerca de la cantidad monetaria mencionada en la política. Esta podría fácilmente haber sido otro monto.

Políticas Relacionadas: “[Programas de Aplicación de Usuarios Finales](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Re-Usabilidad del Software

Política: Todos los proyectos de desarrollo interno con presupuesto por encima de \$ 100.000, deben tener como meta secundaria el desarrollo de software modular confiable que pueda ser introducido en un repositorio de software compartido.

Comentario: El desarrollo y utilización de módulos compartidos normalizados no solamente reduce costos, sino que disminuye el riesgo de errores y de exposiciones inadvertidas de seguridad. Esta política asegura que todos los esfuerzos grandes de desarrollo interno de software produzcan código que pueda ser reutilizado en el futuro. Algunas organizaciones pueden querer añadir determinados requisitos de documentación a esta política de manera que otros desarrolladores puedan entender lo que los desarrolladores originales realmente hicieron. Pueden especificarse dentro de la política otros prerequisitos para la inserción dentro del software de reposición. La política podría también incluir algunas palabras para urgir a los desarrolladores a que utilicen módulos almacenados en un repositorio cuando lo consideren pertinente. Esta política alienta a los desarrolladores a pensar en dividir su código en módulos lógicamente diferentes de forma tal que algunos de estos módulos puedan entrar en un repositorio. Esta clase de política se ha vuelto sumamente importante debido a que las herramientas de ingeniería de software asistida por computación y los ambientes orientados a objetos, son cada vez más ampliamente

utilizados. No existe nada en especial acerca de la cantidad monetaria mencionada en la política. Esta podría fácilmente haber sido otro monto.

Políticas Relacionadas: “[Migración de Software](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas

Política: Para todos los sistemas de aplicaciones de negocios, los diseñadores y desarrolladores de sistemas deben considerar la seguridad desde el principio del proceso de diseño de los sistemas, hasta su conversión en sistemas de producción.

Comentario: A pesar de que es deseable la consideración temprana en el proceso de desarrollo debido a que se considera más eficiente y efectiva, no debe ser el final del proceso de selección de controles. Generalmente, el ciclo de vida del desarrollo de sistemas involucra varios puntos dentro del proceso en los que debe incluirse formalmente la seguridad. En dichos puntos, podrán requerirse firmas a mano, o quizás firmas digitales, que indicarían la suficiencia del trabajo de seguridad. Esta política requiere que el personal técnico considere la seguridad como una parte formal del ciclo de vida del desarrollo de sistemas (SDLC, por sus siglas en inglés). Esta política asume que existe un SDLC reforzado. Este podría no ser el caso en los ambientes de computadores personales, estaciones de trabajo, cliente-servidor, intranet, y redes de área local.

Políticas Relacionadas: “[Especificaciones para Software Desarrollado Internamente](#),” “[Proceso de Control de Cambios para Aplicaciones de Negocios](#),” y “[Convenciones en Desarrollo de Sistemas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Dependencia de Mecanismos Comunes para los Controles

Política: Deben seleccionarse y diseñarse controles de seguridad informática de costo justificado, de forma tal que se minimice la dependencia de un mecanismo común.

Comentario: Si un mecanismo común es utilizado por muchos controles, su falla o no disponibilidad tendrá serios efectos sobre toda la seguridad. Por ejemplo, si un

único nodo en una red fuese el único proveedor de servicios de control de acceso, entonces la no disponibilidad de este nodo podría hacer que toda la red no estuviera disponible. Esta política instruye a los diseñadores de sistemas y demás personal técnico a que eviten estos diseños vulnerables. Como mínimo, la política requiere que los diseñadores de sistemas se pregunten acerca de la dependencia de un mecanismo común. Algunos lectores pueden desear incluir en la política la definición de mecanismo común. Una definición podría ser: “un componente de los sistemas que provee servicios de seguridad a varios sistemas”. Esta política a menudo se encuentra en oposición a los objetivos de diseño de sistemas, como la simplicidad y el costo. Una parte del trabajo del especialista en seguridad informática es conseguir un balance entre estos objetivos contrapuestos. El ámbito de la política podría expandirse para incluir todos los componentes de los sistemas y no solamente los controles.

Políticas Relacionadas: “[Sistemas de Seguridad Independientes](#),” “[Normas de Implantación de Controles](#),” e “[Intervención Humana en Procesos Asistidos por el Computador](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Funcionalidad de la Seguridad en las Aplicaciones del Negocio

Política: Siempre que sea factible y eficaz en función de costos, los desarrolladores de sistemas deben confiar en los servicios del sistema para la funcionalidad de la seguridad en lugar de incorporar dicha funcionalidad en las aplicaciones.

Comentario: Esta política garantiza que los desarrolladores de sistemas internos emplearán la funcionalidad normalizada en seguridad, como el proceso de inicio de sesión asociado con los sistemas operativos. Si los desarrolladores escriben sus propias versiones, estas rutinas comúnmente no serán probadas, documentadas ni soportadas adecuadamente en el futuro. Al insistir en que los todos los desarrolladores utilicen los servicios del sistema, se puede mantener un nivel consistente de seguridad sobre una base de aplicaciones cruzadas. Las mejoras a los servicios de seguridad serán más fáciles de integrar con las aplicaciones. Numerosas rutinas de seguridad propias construidas dentro de aplicaciones pueden evitar que una organización utilice la última versión de un sistema operativo o al menos hacerlo inmanejables, desde el punto de vista administrativo. Existirán ciertas funciones que no se pueden lograr con

los servicios del sistema, y éstas son realizadas mejor a nivel de la aplicación. Por ejemplo, una rutina que lleva a cabo una verificación de errores de entrada generalmente se ejecuta a nivel de aplicación. Esta política funciona mejor si existe una revisión formal y un proceso de aprobación asociado con los esfuerzos de desarrollo, en cuyo caso pueden identificarse las desviaciones frente a esta política. La política también funciona mejor si la organización tiene un conjunto de rutinas de software de seguridad aprobadas que han sido probadas, documentadas y que están disponibles para los desarrolladores.

Políticas Relacionadas: “Controles de Acceso al Sistema de Computación” y “Proceso de Control de Cambios para Aplicaciones de Negocios”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Compra de Soluciones de Seguridad Informática

Política: La Empresa X debe adquirir soluciones de seguridad informática disponibles comercialmente en lugar de construirlas internamente, a menos que la efectividad en función de los costos de la solución interna sea claramente analizada, documentada y aprobada por la gerencia de Seguridad Informática.

Comentario: Esta política ahorra dinero y permite que el personal se enfoque en los problemas del negocio en lugar de dedicarse a los problemas de desarrollo de sistemas de seguridad informática. Las soluciones disponibles comercialmente son generalmente más económicas que las soluciones internas. Las soluciones comerciales generalmente han sido probadas más extensamente, están más documentadas y están más dispuestas a ser modificadas en respuesta a las más recientes amenazas, y son más capaces de proveer una seguridad superior. Sin embargo, en algunos casos, si ningún producto comercial puede satisfacer las necesidades internas, será necesario desarrollar soluciones internas. Aun en estos casos, es factible a menudo unir una solución interna que incorpore varios productos comerciales. Algunos pueden desear extender esta política para que se pueda aplicar a todas las soluciones de sistemas informáticos.

Políticas Relacionadas: “Normas de Seguridad Informática Específicas a Cada Industria,” “Procura de Hardware y Software,” y “Requerimientos para el Soporte de Emergencias y Desastres”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

13. Controles Mínimos en Sistemas Informáticos

Política: Como mínimo, todos los sistemas informáticos de la Empresa X deben incluir los controles normales que se encuentran en otras organizaciones que enfrentan circunstancias similares.

Comentario: Esta política hace referencia a la noción legal de "norma de debido cuidado". La norma de debido cuidado define el conjunto mínimo aceptable de controles que se espera que una organización posea, considerando su industria, localización, la naturaleza de sus negocios y demás aspectos de su situación. Esta política pretende mantener a la organización sin problemas porque si no posee los controles normales de debido cuidado, la gerencia de la organización está sujeta a acusaciones de negligencia, ruptura de la responsabilidad fiduciaria y mala praxis profesional en computación. La política requiere que la gerencia considere el único riesgo que enfrenta la organización, solicitando implícitamente una evaluación de riesgo.

Políticas Relacionadas: “Evaluación del Riesgo en los Sistemas de Producción,” “Normas de Implementación de Controles,” y “Revisión de los Controles de los Sistemas Informáticos — Independiente”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

14. Uso de Productos Evaluados

Política: Debe utilizarse un producto de seguridad de sistemas informáticos evaluado oficialmente en lugar de un producto que no haya sido evaluado.

Comentario: Esta política informa a los diseñadores de sistemas que la gerencia requiere productos que hayan sido evaluados por una fuente confiable de prueba. Los productos evaluados han sido documentados y probados de acuerdo con un conjunto de objetivos de seguridad predefinidos. Un grado que indica el nivel de seguridad provisto por el producto ha sido expedido por la agencia evaluadora. Los productos evaluados serán más seguros que aquellos que no lo han sido. La política está escrita de manera que la gerencia pueda tratar la seguridad como una consideración secundaria. Todos los demás requisitos funcionales deben satisfacerse antes de que la seguridad afecte la decisión. Si la gerencia no desea que la seguridad juegue un papel hasta ese punto, podría desear modificar la política. La política asume que los

objetivos de la entidad evaluadora coincidirán cercanamente con los objetivos de seguridad de la organización. Si esto no ocurre entonces esta política puede no ser apropiada.

Políticas Relacionadas:“Normas de Seguridad Informática Específicas a Cada Industria”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

10.02 Seguridad en Sistemas de Aplicaciones

10.02.01 Validación de los Datos de Entrada

1. Transacciones de Entrada en Producción

Política: Cada transacción de entrada presentada a un sistema de producción debe tener asignada un número secuencial o identificador único.

Comentario:Esta política lleva un control adecuado de todas las transacciones de entrada, y facilita la reconciliación de las transacciones de entrada en caso de que se presente un problema o se sospeche que existe un problema. La existencia de un número serial permite que los datos de entrada del computador puedan enlazarse en forma cronológica con los documentos fuente. También asegura que no se dupliquen las transacciones y que no se extravíen. Para reducir su impacto y costo, esta política puede limitarse a determinadas aplicaciones críticas u otras actividades importantes. La política asume que la organización ya ha definido los términos "transacción" y "producción" de una manera clara y no ambigua.

Políticas Relacionadas:“Retención del Documento Fuente,” “Acceso Físico de Trabajadores Cesados,” y “Transacciones Distintas a Producción”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

2. Validación de Datos de Entrada y Manejo de Item Rechazado

Política: Todas las transacciones que deban ingresarse en un sistema multiusuario de producción deben estar sujetas a verificaciones razonables, verificaciones de edición o verificaciones de validación, y las transacciones que no aprueben esta clase de verificaciones deben ser rechazadas con una notificación del rechazo enviada al emisor, corregidas y reenviadas o suspendidas hasta que se haga una posterior investigación.

Comentario:Esta política requiere que la gerencia valide adecuadamente todos los datos que se envían a los sistemas multiusuario. La validación implica someter a los datos a pruebas que demuestren que han sido adecuadamente formateados, definidos y escritos. Por ejemplo, un programa de cuentas por pagar debe rechazar cualquier entrada en el campo de la cantidad que contenga un carácter alfabético. La entrada también debe estar sujeta a estas pruebas antes de que pueda ser colocada en bases de datos de producción, archivos maestros u otros libros y registros de la organización. Si no se lleva a cabo esta validación, erradicar un error que pasa de un sistema a otro puede ser difícil y costoso. Esta política intenta detectar y corregir los problemas de integridad de los datos lo más pronto posible. Más allá de los errores y omisiones, la política también protege indirectamente en contra del fraude, desfalco, sabotaje y demás actos intencionales. Una forma crecientemente popular y potencialmente poderosa de implementar esta política es a través de un diccionario de datos activos. En este caso, el diccionario de datos será llamado en el procesamiento de producción por varias aplicaciones de sistemas para determinar cuáles rutinas de validación de datos de entrada deben ejecutarse. Las definiciones de datos y pruebas son definidas una sola vez a pesar de que se aplican a diferentes aplicaciones. Ejemplos específicos de problemas que fallen esta clase de pruebas de validación incluyen los valores fuera de rango, caracteres inválidos en los campos de datos, datos faltantes o equivocados y datos de control no autorizados o inconsistentes. Esta política puede modificarse para requerir la corrección del problema dentro de un determinado período de tiempo.

Políticas Relacionadas:“Transacciones de Entrada Rechazadas” y “Cronograma de Resolución de Archivos en Suspensión”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

3. Entrada con Doble Tecla de Transacciones Mayores

Política: Todos los procesos de entrada de producción basados en el teclado que involucren cantidades por encima de \$ 1.000 y que inicien una transacción deben incluir la entrada doble de la cantidad.

Comentario: Esta política evita problemas causados por errores de digitación. La política podría, por ejemplo, solicitar al encargado de ingresar datos de entrada en transferencias cablegráficas que introduzca dos veces todos los campos de cantidades por encima de \$ 1.000. Esta política podría requerir que todo el proceso relacionado con esa transacción sea tecleado dos veces. Por ejemplo, el número de cuenta del banco beneficiario debería ser introducido dos veces. A pesar de que ofrece una menor efectividad en la verificación de la integridad de los datos, en algunos ambientes puede ser suficiente que el computador simplemente haga una petición de confirmación. Debido a que es más efectivo, es preferible el enfoque de la entrada dos veces de la cantidad. El ámbito de esta política puede ser reducido a ciertos campos críticos, como por ejemplo la ortografía del nombre del beneficiario de un cheque de más de \$ 1.000. El ingreso de cantidades por encima de \$ 1.000 en una hoja de cálculo o en cualquier otra aplicación que no genere una transacción no se encontrará dentro del ámbito de esta política. Para mayor protección, la política puede expandirse y requerir que la segunda entrada involucre a otro individuo. Esta política asume que la palabra "producción" ha sido definida en otro lugar. La presencia de esta palabra exime muchas situaciones de un solo usuario como el trabajo en un computador personal en el que el análisis informal no está directamente conectado con la aplicación de producción. No hay nada de especial acerca de la cantidad monetaria mencionada en la política. Esta podría fácilmente haber sido otro monto.

Políticas Relacionadas: “Investigación de Errores” y “Errores y Manipulación de Registros”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

4. Originador de Transacciones

Política: Las transacciones que afecten información sensible, crítica o valiosa deben ser iniciadas únicamente por documentos fuente o mensajes computarizados en los que el individuo que las origina o el sistema estén claramente identificados.

Comentario: La habilidad de rastrear transacciones hasta el individuo o el sistema que las originó es crítica para auditorías, argumentaciones, resolución de problemas y demás esfuerzos. Esta política requiere que exista una auditoría para todas las transacciones que afecten información sensible, crítica o valiosa. Algunas organizaciones pueden desear ir más allá de una identificación de la fuente. Esto puede lograrse mediante firmas digitales, códigos de autenticación de mensajes, cifrado y firmas a mano. La política asume que los términos "sensible, crítica y valiosa" ya han sido definidos en otro lugar.

Políticas Relacionadas: “Autorización para Transacciones en Sistema de Producción,” “Clasificación de Datos en Cuatro Categorías,” “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” y “Firmas en Correo Electrónico”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.02.02 Control de Procesamiento Interno

1. Modificación de la Información de Negocio de Producción

Política: Deben establecerse los privilegios de manera que los usuarios de los sistemas no puedan cambiar los datos de producción de manera irrestricta.

Comentario: Esta política garantiza que no se efectuarán cambios no autorizados en los datos de producción. Esta política indica que deben existir determinados caminos bien controlados a través de los cuales se modifiquen los datos de producción y que

estos datos ya mencionados no deben alterarse a menos que se empleen esos caminos. Por ejemplo, una base de datos debe ser solamente modificada si se emplea el sistema de administración de base de datos asociado (DBMS, por sus siglas en inglés). En este ejemplo, existen determinados controles construidos dentro del DBMS, como las restricciones de privilegios, mientras que es poco común que existan controles dentro de un programa de propósito general que permita que los usuarios modifiquen los archivos en diferentes formatos.

Políticas Relacionadas:“Privilegios Sobre la Información de Producción” y “Separación de Tareas”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

2. Falla de Operación del Software

Política: Cada vez que el software desarrollado internamente falle y no produzca los resultados esperados, siempre debe proporcionar un mensaje de error o alguna otra indicación de falla como respuesta al operador.

Comentario:Es peligroso que el software produzca resultados erróneos, particularmente cuando los usuarios confían en esos resultados para sus actividades de negocios. Por ejemplo, si un programa no puede aceptar nuevos datos de entrada, podría automáticamente utilizar los últimos datos que se ingresaron. Esta diferencia en los datos de entrada podría no ser detectada por el usuario. Sin una notificación específica del problema, el usuario podría tomar decisiones equivocadas en base a información inexacta. Esta política asegura que los usuarios estén siempre conscientes de fallas en el software interno. Esta política compensa parcialmente el hecho de que muchos usuarios aceptan los reportes generados por computador sin un mayor análisis, asumiendo que son correctos. El software provisto externamente generalmente incluye la notificación de errores, a pesar de que esta política podría extenderse e incluir al software externo. Si este cambio en la política se hiciera, entonces podría utilizarse para la toma de decisiones en la adquisición de software. Esta política implícitamente requiere que los desarrolladores internos incorporen verificaciones razonables en el software que construyen. Esta es la única manera de saber si el software produjo los resultados esperados.

Políticas Relacionadas:“Retroalimentación del Software al Usuario” y “Mantenimiento Preventivo”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

3. Retroalimentación del Software al Usuario

Política: Cada vez que el software desarrollado internamente reciba una entrada del usuario, debe dar respuesta indicando si se llevó a cabo la solicitud.

Comentario:Puede haber confusión cuando los usuarios piensan que han instruido al sistema a llevar a cabo determinada acción, cuando en realidad no lo han

hecho. Por ejemplo, cuando se utiliza un cajero automático, el cliente puede pensar que solicitó al sistema transferir cierta suma de dinero de su cuenta de ahorros de mercado de valores a su cuenta corriente. En lugar de esto, pudo haber presionado una tecla equivocada, solicitando que la cantidad fuera transferida de su cuenta de ahorros. Si el cliente no posee una cuenta de ahorros, entonces el cajero podría simplemente ignorar la entrada. Si no responde con un mensaje de error, el cliente podría asumir que se ha efectuado la transferencia. Esta política requiere que los diseñadores de sistemas siempre redacten mensajes de error que indiquen que el sistema no pudo llevar a cabo la solicitud, si ése es el caso. Esta política también requiere una confirmación cuando la entrada es aceptable. La política también podría aplicarse a todo el software a pesar de que generalmente es muy difícil que el personal interno pueda hacer modificaciones o colocar parches a paquetes de software escritos por terceros.

Políticas Relacionadas:“Falla de Operación del Software”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

4. Interrupción del Sistema por Seguridad

Política: Los robots y otras máquinas computarizadas deben ser programados de manera que la actividad actual se detenga inmediatamente si está dañando o es factible que dañe a una persona.

Comentario:Esta política es aplicable a los procesos de control de sistemas, cintas de transporte, líneas de ensamblaje y demás sistemas computarizados similares. La intención de la política es que se requiera a los diseñadores que consideren las circunstancias en las que el sistema podría amenazar la seguridad humana. La política podría expandirse e incluir una notificación inmediata al operador sobre la condición de peligro. Una política como ésta puede ser útil cuando se quiere demostrar que el sistema ha sido diseñado considerando la seguridad humana. Esto podría ser útil al defenderse de demandas que aleguen negligencia. Esta política también puede mejorar las relaciones entre la gerencia y los empleados debido a que demuestra la preocupación por la seguridad del empleado.

Políticas Relacionadas:“Contraseñas de Presión” e “Intervención Humana en Procesos Asistidos por el Computador”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos**5. Seguimiento de Errores y Problemas de Seguridad por Desarrolladores**

Política: Todas las quejas sobre errores en el software, omisiones y problemas de seguridad que puedan ser atribuibles al software desarrollado internamente deben poder ser rastreadas hasta los diseñadores, programadores y demás personal involucrado en su desarrollo.

Comentario: Esta política anima al personal de desarrollo a considerar seriamente la seguridad al momento de diseñar un sistema de software nuevo o mejorado. Estos integrantes del personal técnico se encuentran a veces bajo mucha presión por entregar un programa que trabaje razonablemente bien, en base a plazos de tiempo poco realistas. Para poder cumplir con estos plazos, por lo general ignoran la seguridad; y sus elecciones en esta materia por lo general están apoyadas por el personal de la gerencia de proyectos. Esta política da un sentido de responsabilidad por los problemas que pueden presentarse en el futuro. Si los miembros del personal de desarrollo están conscientes de que serán responsables de problemas futuros, le darán un nuevo nivel de profesionalismo y se preocuparán por los aspectos relacionados con la seguridad en el trabajo que llevan a cabo. Esta política también indicará aquellos lugares en los que el proceso de desarrollo falla y requiere reparación. Nótese que las palabras "personal involucrado en su desarrollo" no se refieren únicamente a los empleados. Estas palabras incluyen contratistas, consultores y empleados temporales.

Políticas Relacionadas: "[Proyectos que Involucran Seguridad Humana](#)" y "[Originador de Transacciones](#)"

Política Dirigida a:Personal técnico**Ambientes de Seguridad:**Todos**6. Cambios en la Sensibilidad, Criticidad y Valor de la Información**

Política: Las transacciones que afecten información sensible, crítica y valiosa deben ser procesadas únicamente si el iniciador o el sistema está autorizado para procesar dichas transacciones.

Comentario: Esta política requiere que la gerencia establezca y mantenga un sistema de control de acceso adecuado de manera tal que únicamente los usuarios autorizados puedan modificar información sensible,

crítica o valiosa. La forma más frecuente de hacer esto es a través de contraseñas fijas, a pesar de que las contraseñas dinámicas rápidamente se están convirtiendo en la norma para los computadores con marcado y conexión a Internet. La verificación de la autorización también puede hacerse utilizando tarjetas inteligentes, firmas digitales en mensajes de correo electrónico, comparaciones de códigos de autentificación de mensajes para instrucciones de transferencias cablegráficas y certificados digitales. La política asume que los términos "sensible, crítica y valiosa" ya han sido definidos en otro lugar.

Políticas Relacionadas: "[Autentificación de Usuario Que Accede Vía Teléfono](#)," "[Clasificación de Datos en Cuatro Categorías](#)," "[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#)," y "[Autentificación del Usuario por el Sistema Operativo](#)"

Política Dirigida a:Personal técnico**Ambientes de Seguridad:**Todos**7. Validación de los Controles**

Política: Antes de utilizar todos los datos financieros que sean críticos para la toma de decisiones que involucren más de \$ 100.000, los datos deben ser verificados en forma cruzada mediante controles totales, registros de cuentas o controles similares.

Comentario: Esta política garantiza que los datos utilizados para la toma de decisiones importantes serán confiables y estarán completos y documentados adecuadamente. La política requiere que se soporten datos que sean validados con medidas normales de control. La política es particularmente relevante para los computadores personales, estaciones de trabajo y otros computadores pequeños como los sistemas cliente-servidor, debido a que esa clase de controles por lo general se olvidan en este tipo de ambientes informales de computación. Por ejemplo, un usuario puede haberse equivocado al escribir los datos de entrada en una hoja de cálculo y esto podría no determinarse a menos que se empleen controles como los que se mencionan en la política. La noción de "criticidad" debe también ser definida para que esta política pueda ser comprendida completamente. No existe nada en especial acerca de la cantidad monetaria mencionada en la política. Esta podría fácilmente haber sido otro monto y debe basarse en el grado de riesgo que la organización desea aceptar.

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” “Validación Cruzada de la Información,” y “Revisión de Análisis Computarizados”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Transacciones de Entrada Rechazadas

Política: Todas las transacciones de entrada rechazadas deben ser colocadas en un archivo en suspenso e incluidas en reportes de excepción hasta que hayan sido reenviadas exitosamente para su procesamiento o resueltas de otra manera.

Comentario: Esta política especifica un método normal para manejar las transacciones rechazadas de forma que todas las transacciones puedan ser procesadas rápidamente. Un archivo en suspenso es un área donde se mantienen los ítems rechazados. Los archivos en suspenso deben ser resueltos diariamente y aquellos ítems que no sean resueltos deben someterse a un escrutinio adicional de la gerencia. La gerencia debe brindar especial atención a la rápida resolución de las razones por las que ciertas transacciones han sido rechazadas. Si no lo hace, los archivos en suspenso pueden ser utilizados para perpetrar fraude y otros actos no autorizados. Puede ser deseable expandir la política para que requiera una purga periódica de los archivos en suspenso.

Políticas Relacionadas: “Cronograma de Resolución de Archivos en Suspensión” y “Validación de Entrada Rechazada o Suspendida”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Cronograma de Resolución de Archivos en Suspensión

Política: Todas las transacciones de entrada que se mantienen en estatus de suspensión en espera de una investigación deben ser o reenviadas o manejadas dentro de un plazo de 10 días hábiles a partir de su ingreso original.

Comentario: Esta política garantiza que todos los ítems rechazados serán rápidamente resueltos. Si esto no se hace, pueden presentarse fraudes u otros actos no autorizados. El lapso de tiempo será generalmente mucho menor en el caso de un banco, mientras que

puede ser mayor en el caso de una agencia gubernamental. En algunos casos puede ser necesaria una autorización para mantener un ítem en un archivo en suspenso durante un lapso mayor que el especificado.

Políticas Relacionadas: “Transacciones de Entrada Rechazadas” y “Validación de Entrada Rechazada o Suspendida”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10. Ocultar Números de Cuenta de Clientes

Política: Los números de cuenta que aparecen en los recibos generados por computador que se entregan a los clientes deben ser parcialmente ocultados o truncados.

Comentario: Esta política evita que terceros no autorizados utilicen la información que se imprime en recibos descartados o extraviados para cometer fraude. Al mismo tiempo, si se provee información parcial de la cuenta, los clientes podrán determinar cuál de sus cuentas estuvo involucrada en la transacción. Esta política cumple con los objetivos de prevención de fraude y buen servicio al cliente. Uno de los ejemplos más predominantes de esto se refiere a los comprobantes de transacciones de cajeros automáticos. En estos comprobantes, el número de la tarjeta de débito para un avance de efectivo debe tener algunos dígitos ocultos. En el caso de recibos de tarjetas de crédito, debe ocultarse la fecha de expiración deliberadamente. Esta política no es relevante en transacciones en donde el recibo es un documento fuente para una posterior entrada en el computador. Por ejemplo, esta política no es apropiada para recibos hechos a mano por compras con tarjeta de crédito, porque todo el número de la tarjeta será necesario para completar la transacción o para que sirva de referencia a la misma. Sin embargo, la política es adecuada en el caso de transacciones que han sido registradas en el sistema informático o que ya se han completado. El ocultamiento parcial que se menciona puede conseguirse enmascarando una parte del número de cuenta con otros caracteres como la “X”.

Políticas Relacionadas: “Divulgación del Registro de las Actividades del Cliente,” “Diseminación Secundaria de la Información Secreta,” y “Entrega de Información Secreta”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Entrega de Recibo de Compra

Política: Un aviso que indique que "los clientes que no reciban su comprobante no pagarán por su compra" debe ser colocado de manera destacada en todas las cajas registradoras.

Comentario: Esta política evita que los cajeros tomen dinero de manera furtiva de las cajas registradoras. Este control requiere que toda transacción sea ingresada en la caja registradora. Si a los cajeros se les permitiera aceptar dinero por las transacciones, sin ingresararlo en la caja registradora, podrían fácilmente guardarse el dinero sin ser descubiertos. Esta política requiere que el dinero recogido por el cajero al finalizar su turno coincida con la cantidad indicada en la caja registradora. La provisión de bienes gratuitos hace que el cliente se motive y forme parte de este sistema interno de control. La ubicación destacada de un aviso en donde se describa este arreglo es necesaria si el cliente va a ser notificado de su participación en este sistema de control interno. Una división similar de responsabilidades puede ser aplicada a situaciones similares en donde exista el riesgo de robo de dinero, cheques, depósitos u otras formas de dinero. Otra razón importante para entregar comprobantes a los clientes involucra la provisión de un registro autorizado que pueden verificar con sus estados de cuenta mensuales, de manera que se asegure que la contabilidad y otras actividades puedan realizarse adecuada y rápidamente.

Políticas Relacionadas: "[Separación de Tareas](#)" y "[Ocultar Números de Cuenta de Clientes](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Uso de Números de Tarjeta de Crédito

Política: Los números de las tarjetas de crédito no deben ser utilizados para la identificación de los clientes ni para ningún otro propósito excepto el de procesar pagos de bienes o servicios.

Comentario: Mientras más se utilicen los números de las tarjetas de crédito con propósitos diferentes del procesamiento de pagos, es más probable que aparezcan en forma legible en lugares en los que no estarán protegidos adecuadamente. Esto puede llevar a fraude, robo de identidad y otros abusos. En algunos establecimientos al detal, las tarjetas de crédito se utilizan como identificación, por ejemplo para cambiar un cheque. Los dependientes pueden inclusive anotar el número de la

tarjeta de crédito en la parte posterior del cheque, exponiéndolo así a todas las personas que manejan el proceso de cobro del cheque y las actividades contables relacionadas. Esta política establece el punto de partida para la prevención del fraude y del robo de identidad y puede ser útil cuando se quiere demostrar que la organización tomó pasos diligentes para proteger los números de las tarjetas de crédito del uso no autorizado.

Políticas Relacionadas: "[Cifrado de Datos de Pago](#)" y "[Números de Cuenta Bancaria](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

13. Diseño de Controles de Seguridad Informática

Política: Cuando se diseñen controles de seguridad informática, los empleados deben emplear grandes márgenes de error y grandes cantidades de tiempo.

Comentario: Esta política refuerza el hecho de que el diseño de sistemas de seguridad informática debe incorporar márgenes significativos de error y grandes cantidades de tiempo. Esta política reconoce que los sistemas construidos actualmente pueden ser utilizados dentro de una década o mucho después. Esta política también se refiere a desarrollos inesperados, como por ejemplo nuevas técnicas matemáticas que hagan el análisis más fácil y rápido. Esta clase de desarrollo inesperado puede significar que los sistemas de cifrado existentes pueden comprometer al sistema a pesar de que no lo comprometieran en el pasado reciente. Esta política no solamente es relevante en el caso de la longitud de la clave de cifrado. También se aplica a la longitud de las contraseñas fijas, la longitud del generador de números aleatorios y otros parámetros de seguridad. Esta política encara directamente la tendencia a minimizar costos, que si se utiliza como un factor principal en la toma de decisiones, en muchos casos puede llevar a que los sistemas de seguridad informática sean obsoletos o débiles en un corto lapso de tiempo.

Políticas Relacionadas: "[Errores y Manipulación de Registros](#)" y "[Dependencia de Mecanismos Comunes para los Controles](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

14. Intervención Humana en Procesos Asistidos por el Computador

Política: Todos los procesos asistidos por computador deben involucrar la intervención humana antes de iniciar cualquier acción que pueda resultar en una amenaza a la vida o a la seguridad humana.

Comentario: Esta política evita que los diseñadores de sistemas otorguen decisiones importantes a los computadores. Por ejemplo, los disparadores de algunos sistemas de proyectiles requieren que dos personas autorizadas los inicien simultáneamente. No pueden iniciarse mediante un acto del computador sin la intervención humana. La referencia a las situaciones de "amenaza a la vida" y "amenaza a la seguridad" pueden expandirse e incluir decisiones financieras significativas y decisiones que puedan impactar significativamente otras áreas. No se hace ninguna mención a sistemas expertos, redes neurálgicas, inteligencia artificial u otra tecnología específica.

Políticas Relacionadas: “Dependencia de Mecanismos Comunes para los Controles” e “Interrupción del Sistema por Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

15. Errores y Manipulación de Registros

Política: Los sistemas de computación de la Empresa X deben ser construidos de manera que ninguna persona pueda cometer un error o manipular los registros sin que esos eventos sean detectados por otra persona durante la ejecución rutinaria de sus responsabilidades.

Comentario: Esta política es una expresión orientada a la detección del principio de división de responsabilidades. En lugar de enfocarse en la prevención de problemas, toma un enfoque menos estricto en el que se requiere que sólo los errores y manipulaciones sean descubiertos. Este enfoque puede involucrar pocos o menos costosos controles que un enfoque preventivo más estricto, y por lo tanto puede ser atractivo para las empresas pequeñas. A largo plazo, los costos totales generalmente serán mayores de lo que serían dentro de un enfoque preventivo.

Políticas Relacionadas: “Separación de Tareas,” “Entrada con Doble Tecla de Transacciones Mayores,” e “Investigación de Errores”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

16. Archivos y Almacenamiento Temporales

Política: Los archivos temporales y las ubicaciones de almacenamiento temporales dentro de la memoria de los computadores de propósito general, deben ser sobreescritos cuando el proceso programado que los creó haya completado su trabajo.

Comentario: Esta política garantiza que la información sensible como las contraseñas y claves de cifrado no serán divulgadas inadvertidamente por terceros no autorizados. La información sensible a menudo es escrita en un archivo temporal o en ubicaciones temporales de memoria para completar una aplicación. Esta política instruye a los programadores y diseñadores de sistemas en el sentido de que esta información debe ser reescrita antes de que se complete el proceso programado. No es suficiente borrar o eliminar esta información debido a que en muchos computadores, estos comandos simplemente borran la referencia a los datos pero no destruyen la información en sí. Esto significa que la información está disponible para personas que puedan escudriñar el sistema. Utilizando programas utilitarios de reparación del disco, por ejemplo, se puede revelar información que ha sido borrada o eliminada del disco duro. Los procesos de reescritura repetidos también son recomendables debido a que con esta repetición puede superarse el registro de datos residuales.

Políticas Relacionadas: “Apagado de Computadores,” “Certificado de Destrucción de Medios de Almacenamiento,” y “Materiales para la Generación de Contraseñas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

10.02.03 Autentificación de Mensajes

1. Autorización para Transacciones en Sistema de Producción

Política: Deben existir métodos que aseguren que todas las entradas a los sistemas de producción que han sido enviadas para su procesamiento hayan sido autorizadas adecuadamente.

Comentario: Esta política preserva la integridad de los libros o registros de la Empresa X. Si se colocan transacciones no autorizadas en los libros o registros, éstos pueden volverse cuestionables. Esta política previene el fraude, desfalco, sabotaje y un número de actos abusivos que pueden ser perpetrados por personas que tenían acceso al sistema informático pero que no poseían una autorización adecuada. La autorización puede tomar la forma de un documento fuente para verificación de la firma, firmas digitales para mensajes de correo electrónico y códigos de autentificación de mensajes para transferencias cablegráficas. Una de las maneras más comunes de indicar autorización es utilizar una contraseña secreta.

Políticas Relacionadas: “[Autorización para Transacciones de Producción](#)”, “[Cambios en Producción](#)” y “[Originador de Transacciones](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Validación de Entrada Rechazada o Suspendida

Política: Las transacciones de entrada corregidas y reenviadas, o aquellas suspendidas y posteriormente aprobadas para ser reenviadas, deben estar sujetas a los mismos procedimientos de validación que las transacciones de entrada originales.

Comentario: Esta política requiere la aplicación uniforme de controles para todas las transacciones de entrada. Si no se utilizan los mismos procedimientos de validación para aquellos ítems que fueron rechazados o suspendidos, existe una vulnerabilidad en la seguridad. Esto se debe a que las personas que manejan los ítems pueden rechazar o suspender uno, modificarlo y reenviarlo. Si no se utilizan las mismas verificaciones para validarlos, el ítem modificado puede evadir medidas importantes de control. Más allá del fraude y del desfalco, esta vulnerabilidad puede también llevar a una degradación de la integridad de la información. Esta política es consistente con los procedimientos normales de prueba para el software que requieren que se realicen todas las verificaciones nuevamente en caso de que exista una modificación en el código subyacente. Estos procedimientos de prueba reconocen la complejidad del ambiente de computación y el hecho de que las personas se equivocan al no ver las consecuencias asociadas con modificaciones menores.

Políticas Relacionadas: “[Prueba del Software](#)” y “[Transacciones de Entrada Rechazadas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.02.04 Validación de Datos de Salida

1. Controles de Datos de Salida

Política: Deben establecerse controles y procedimientos para validar toda la información sensible o crítica procesada por los sistemas de aplicaciones de la Empresa X.

Comentario: Esta política garantiza que todos los datos de salida de los sistemas de procesamiento de la Empresa X han sido validados por un proceso efectivo y rutinario. Si bien los sistemas son generalmente validados, verificados y probados, no existe seguridad

de que la información procesada en ellos sea correcta. Por ejemplo, deben implementarse procesos que ejecuten verificaciones de plausibilidad o que reconcilien cuentas de control. También debe haber procedimientos establecidos que definan las responsabilidades de aquellos que están involucrados en el proceso de validación de las salidas. Deben documentarse las políticas para cada uno de estos procesos para asegurar que se les dé el adecuado nivel de atención y que sean revisados en forma rutinaria por autoridades de examen.

Políticas Relacionadas:“[Validación de Datos de Entrada y Manejo de Item Rechazado](#)” y “[Validación de Entrada Rechazada o Suspendida](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

2. Revisión de Cambios a Registros Internos

Política: La gerencia debe revisar o establecer mecanismos para que personas responsables y adecuadamente calificadas revisen la racionalidad y exactitud de todos los cambios en los registros internos.

Comentario:Esta política requiere que todas las actualizaciones a los registros de la Empresa X sean revisadas por la gerencia o por un delegado de la gerencia que esté adecuadamente autorizado. A menudo esta política

forma parte de la cultura organizacional en las compañías de comercialización y se vuelve superflua. Esto se debe a que las normas de seguridad tienen los más exigentes requisitos para todas estas actividades de revisión. Para compañías más pequeñas, organizaciones sin fines de lucro y agencias gubernamentales, esta política puede ser justificable. Las verificaciones razonables son generalmente hechas a través de un análisis proporcional, reconciliación y procedimientos similares. Las verificaciones de exactitud se realizan a través de inventarios físicos y pasos similares de revisión.

Políticas Relacionadas:“[Revisión de Registros del Sistema](#)”

Política Dirigida a:Gerencia

Ambientes de Seguridad:Todos

10.03 Controles Criptográficos

10.03.01 Política Sobre el Uso de los Controles Criptográficos

1. Versiones de Software para Firmas Digitales y Cifrado de Archivos

Política: Los usuarios deben retener copias de respaldo de todas las versiones del software utilizado para producir firmas digitales y para cifrar archivos.

Comentario:Esta política garantiza que los usuarios comprenderán que deben mantener copias confiables de todo el software utilizado para generar o verificar firmas digitales, o el utilizado para cifrar o descifrar archivos. De lo contrario, se pone en riesgo la posibilidad de que el usuario pueda demostrar que firmó un archivo, y esto puede dañar su posición en un tribunal, en procedimientos de arbitraje o en un proceso de mediación. Por otra parte, de no hacerlo, también se pone el riesgo la

posibilidad de que pueda recuperar un archivo que fue previamente cifrado. Esta puede parecer una tarea difícil si los usuarios mantienen individualmente un archivo de software. Idealmente, esto debería hacerse en forma centralizada por el administrador del sistema que también maneja la distribución automatizada de software asociada con nuevas versiones del mismo software.

Políticas Relacionadas:“[Ciclo de Vida de las Claves Privadas de Firmas Digitales](#)” y “[Controles para Modificaciones de los Registros del Sistema](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Medianos y altos

10.03.02 Cifrado

1. Autorización del Proceso de Cifrado — Sistemas

Política: Los procesos de cifrado no deben ser utilizados para la información de la Empresa X, a menos que los procesos sean aprobados por la gerencia de Seguridad Informática.

Comentario:Esta política evita que los usuarios dañen o destruyan la información de la Empresa X por no poseer la experiencia o el conocimiento requerido para utilizar adecuadamente las facilidades de cifrado. Únicamente después de que la gerencia de Seguridad Informática se encuentra satisfecha de que existen los controles adecuados para recuperar la información, debe aprobar el uso del cifrado. Uno de los mejores controles

para el cifrado es que la gerencia pueda evadir las claves, de manera tal que se le permita descifrar la información aún si una clave se ha extraviado, traspapelado o se ha escondido intencionalmente. Estas también se denominan facilidades de "custodia de clave" o de "recuperación de clave". Uno de los mayores riesgos que enfrenta una organización cuando permite que el personal utilice el cifrado es que una vez que la información importante sea cifrada, la clave pueda ser recuperada por el personal. La política también pretende asegurar que únicamente los algoritmos aprobados, modos de operación y demás aspectos de los procesos de cifrado cumplan con las normas internas. Si todos los usuarios pudieran libremente hacer lo que quisieran, la actividad resultante interferiría con la comunicación segura de información confidencial o privada. En algunas jurisdicciones, el cifrado es ilegal, o puede requerirse que la clave sea descubierta a las agencias gubernamentales. Para asegurar que los usuarios no incumplan la ley inadvertidamente, la gerencia de Seguridad Informática debe estar involucrada en la decisión de utilizar el cifrado.

Políticas Relacionadas:“[Armamentos en Comercio Internacional](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

2. Autorización de Proceso de Cifrado — Usuarios

Política: Los usuarios no deben emplear el cifrado, las firmas digitales o los certificados digitales en ninguna de las actividades de negocios o información de negocios de la Empresa X sin la autorización escrita del jefe de su departamento, sin la finalización de un adecuado adiestramiento y sin que personal autorizado haya configurado sus sistemas.

Comentario: Esta política pretende evitar que los miembros del personal tengan problemas al cifrar un archivo, porque pueden perder la clave y borrar la versión legible. La política requiere que todos aquellos que vayan a utilizar estos procesos tengan aprobación de la gerencia, estén entrenados y por último que sus sistemas estén adecuadamente configurados. Esta política evita el uso de estas herramientas nuevas hasta que se haya establecido la necesidad y se hayan cumplido otros prerrequisitos. Sin este enfoque, son grandes las posibilidades de que los usuarios descarguen programas de cifrado de Internet e intenten hacerlo ellos mismos. Esta política también permite que se borre del

disco duro software de cifrado que sea descubierto mediante rutinas de auto-descubrimiento. Esto puede llevarse a cabo en forma automática y puede garantizar que los usuarios no están utilizando estas herramientas. También asegurará que los datos críticos no serán cifrados maliciosamente para mantenerlos fuera del alcance de aquellos que los necesitan.

Políticas Relacionadas:“[Autorización del Proceso de Cifrado — Sistemas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

3. Contraseñas y Claves en Utilidades de Cifrado

Política: Los empleados nunca deben emplear programas utilitarios de cifrado que soliciten que el usuario ingrese una contraseña o clave de cifrado.

Comentario: Esta política procura mantener la información perpetuamente disponible para actividades de negocios. La política establece que la gerencia no debe correr el riesgo de que la contraseña o clave ingresada por un usuario se pierda, se olvide o se esconda deliberadamente. Esta política permite que el software de auto descubrimiento se utilice para detectar la existencia de programas utilitarios de cifrado. Si se utiliza un sistema de administración de cambios en un computador personal, un programa utilitario de cifrado puede inclusive borrarse del disco duro del usuario a través de comandos remotos iniciados por el administrador del sistema. Muchos paquetes de procesamiento de palabras incluyen características de cifrado. Algunas organizaciones pueden querer desactivar estas características. Es deseable que los usuarios no sean capaces de controlar exclusivamente los datos de la organización. Esta política pretende evitar esta peligrosa situación. La política no evita el uso de programas utilitarios de cifrado transparentes al usuario que están incrustados en las redes. Aquellos negocios que posean datos particularmente sensibles necesitarán programas utilitarios de cifrado controlados por el usuario. Para ellos, será una opción preferible tener sistemas de custodia de claves, administrados por un empleado.

Políticas Relacionadas:“[Autorización del Proceso de Cifrado — Sistemas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Low

4. Algoritmo de Cifrado Normal e Implantación

Política: Si se utiliza el cifrado, deben emplearse algoritmos normales aprobados por el gobierno y las implantaciones normalizadas.

Comentario: Esta política requiere que todos los sistemas dentro de una organización empleen los mismos algoritmos de cifrado y las mismas implantaciones de sistemas de cifrado. Esta política ayudará a asegurar la interoperabilidad que reducirá costos y facilitará las comunicaciones de negocios seguras. Esta política también asegurará la conformidad con las leyes gubernamentales y las regulaciones y permitirá que se utilice el cifrado en situaciones en las que de otra manera sería ilegal. Por ejemplo, el tráfico cifrado en una red internacional puede ser ilegal de acuerdo con las leyes de cierto país, pero estas leyes pueden ser menos severas si se utilizan algoritmos e implantaciones gubernamentales normalizadas y si se siguen determinados procesos de aprobación.

Políticas Relacionadas: “[Procura de Hardware y Software](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

5. Algoritmos de Cifrado Evaluados Públicamente

Política: Todo algoritmo de cifrado de propósito general utilizado para proteger la información de producción de la Empresa X y sus sistemas informáticos debe ser divulgado públicamente y debe haber sido evaluado por expertos criptográficos.

Comentario: Esta política evita que las organizaciones tengan problemas al crear sistemas de cifrado inseguros o adquieran de un proveedor un algoritmo patentado débil. La criptografía es muy compleja y es difícil hacerla correctamente. Esta política garantiza que expertos estarán involucrados en el trabajo de diseño criptográfico, mientras que varias otras personas pueden estar involucradas en la implementación de los sistemas que desarrollaron dichos expertos. Esto significa que las organizaciones adquirirán módulos que han sido escritos por proveedores de cifrado. Algunas personas argumentan en contra de esta política que la confidencialidad hará más difícil el descifrado del sistema. Pero nada evita que una organización use algoritmos abiertos mientras que no divulgue cuáles algoritmos emplea. Este enfoque provee la certeza de que el algoritmo ha sido evaluado y es fuerte, pero al mismo tiempo debido

a que la implantación se mantiene confidencial, se necesita más esfuerzo para romper el código. Las palabras "propósito general" se añadieron a la política para excluir los algoritmos de cifrado construidos dentro de los sistemas de seguridad.

Políticas Relacionadas: “[Algoritmo de Cifrado Normal e Implantación](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Inicialización del Sistema de Cifrado

Política: Siempre que se inicialice, instale, active o reinicie un sistema de cifrado que se utilizará en los sistemas informáticos de producción de la Empresa X, debe estar presente un especialista auditor de computación.

Comentario: Si bien se pueden hacer muchas cosas para limitar el daño que una persona puede hacer a los sistemas de una organización, la gerencia confía que su personal técnico cumplirá los procedimientos establecidos. Esto es especialmente importante cuando se cargan claves de cifrado en servidores de comercio en Internet y en otros sistemas informáticos de producción sobre los cuales la organización depende en gran medida. La política tiene como objetivo dar a la gerencia una certeza adicional de que el proceso se ha completado de una manera correcta, confiable y segura. La presencia de un auditor producirá un efecto de seriedad sobre aquellos que estén presentes y puede ser importante en caso de que en el futuro se presenten alegatos de negligencia por parte de la gerencia. Se enfoca el proceso de inicialización del sistema debido a que ese es el momento de mayor vulnerabilidad. Después de que se ha establecido el sistema de cifrado, las claves pueden modificarse automáticamente con menor riesgo. Esta política asume que se utilizará un proceso de administración automatizada de claves. Si éste no es el caso, entonces se recomienda la presencia de un auditor en todos los procesos de cambio de claves. La presencia de un auditor también puede ser útil para propósitos de mercadeo y relaciones públicas, al ayudar a establecer un mayor nivel de confianza en el sistema informático involucrado.

Políticas Relacionadas: “[Implantación de Sistemas Multiusuario](#)” y “[Revisión de los Controles de los Sistemas Informáticos — Interno](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

7. Eliminación de Datos Fuente Despues de Cifrar

Política: Cada vez que se utilice el cifrado, los empleados no deben borrar la única versión legible de los datos, a menos que hayan demostrado que el proceso de cifrado puede restablecer una versión legible de los datos.

Comentario: Esta política evita que se pierdan todas las copias de datos sensibles. Sin verificar que el proceso de cifrado funciona, un mal funcionamiento del sistema de cifrado puede significar que la única copia de los datos se pierda para siempre. Algunas organizaciones prefieren el término "texto claro" en lugar de "legible". Una sustitución en la política puede hacerse fácilmente. Algunas organizaciones pueden desear especificar cómo se demuestra que un proceso de cifrado funciona.

Políticas Relacionadas: "Sistemas de Cifrado de Propósito General"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

8. Compresión y Cifrado de Datos Secretos

Política: Si la información secreta debe almacenarse en un sistema de computación multiusuario, debe ser comprimida y posteriormente cifrada utilizando un algoritmo de cifrado aprobado.

Comentario: Al comprimir los datos, se elimina una buena parte de la redundancia de los lenguajes naturales. Esto hace que el trabajo de análisis sea mucho más difícil, lo cual protege la confidencialidad de los datos. Al comprimir y posteriormente cifrar, aumenta la fuerza del proceso de cifrado. Esta política requiere que los diseñadores de sistemas, programadores y demás personal técnico implementen la compresión de los datos con el cifrado, y que especifiquen la secuencia en la que estos procesos deben ser aplicados a los datos. La compresión puede estar enlazada con el cifrado de forma que los dos procesos ocurran simultáneamente, de una manera transparente para el usuario final. Los "algoritmos de cifrado aprobados" serán definidos por cada organización al emitir una política como ésta. La necesidad de soporte y aprobación externa, como por ejemplo de agencias gubernamentales, también puede ser añadida a esta política.

Políticas Relacionadas: "Autorización del Proceso de Cifrado — Sistemas"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Módulos de Hardware para el Proceso de Cifrado

Política: Todos los procesos relacionados con el cifrado deben ser realizados en módulos de hardware no modificables.

Comentario: Los módulos no modificables automáticamente borrarán los datos sensibles, como por ejemplo las claves de cifrado y los vectores de inicialización que se mantienen en la memoria cuando los módulos se abren o se intentan forzar. Estos módulos también son blindados para evitar que las claves y otros datos de seguridad relevantes sean revelados a través de emanaciones electromagnéticas. Esta política requiere que todos los procesos de cifrado sean implementados utilizando equipo especial que aumente la seguridad de los procesos de cifrado. Estos módulos evitan que las claves sean manejadas manualmente, reduciendo las posibilidades de que personas no autorizadas puedan obtenerlas. En algunos ambientes, esta política será difícil y prohibitivamente costosa. Por ejemplo, si se espera que el proceso de cifrado cambie frecuentemente entonces cada nuevo cambio implicará nuevo hardware. En algunos casos los "módulos no modificables" se denominan "módulos de seguridad". Más allá del cifrado, los módulos no modificables también son apropiados para un gran número de procesos de seguridad como los códigos de autentificación de mensajes, la generación de claves de cifrado y la generación de contraseñas seudoaleatorias.

Políticas Relacionadas: "Divulgación de Claves de Cifrado — Controles," "Protección Contra la Radiación Electromagnética," y "Divulgación de Claves de Cifrado — Autorización"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10. Protección de Mensajes Cifrados

Política: Todo contenido enviado a través de la red de datos interna de la Empresa X debe estar cifrado, acompañado de mensajes para desviar la atención y relleno de información ajena para ocultar la longitud de los mensajes enviados.

Comentario: Esta política evita que terceros determinen quién está enviando mensajes a quién y cuál es la longitud de los mensajes. A pesar de que estos mensajes pueden cifrarse, el descubrimiento de esta información

acerca del tráfico de la red, puede descubrir cosas que las partes involucradas nunca pretendieron revelar. Por ejemplo, si se sabe que una organización pequeña tiene problemas financieros y está buscando que una organización más grande la adquiera, y si se interviene la comunicación por Internet, entonces un tercero puede darse cuenta de que existen varios mensajes de tamaño significativo entre la empresa grande y la empresa pequeña. A partir de esta información, este tercero puede deducir que la empresa grande estaba en proceso de negociar la compra de la empresa pequeña. Estas consideraciones son de gran importancia para las agencias militares. La información acerca de quién envía información a quién, cuándo y cuán largos son los mensajes, puede ser utilizada para indicar una maniobra futura. Debido a estas razones, las organizaciones que son muy conscientes acerca de la seguridad pueden desear considerar esta política. Los costos de una red que soporte esta política son bastante altos y justificables únicamente cuando los riesgos son bastante altos.

Políticas Relacionadas: “Esconder Transmisión de la Información” y “Privacidad de Información de Contacto de Remitentes”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

11. Información en Servidores FTP Anónimos

Política: Todos los archivos proporcionados por los usuarios que no hayan sido aprobados explícitamente para su divulgación pública por la gerencia de Mercadeo y que se encuentren residentes en el servidor FTP anónimo de la Empresa X, deben cifrarse utilizando software normal de la Empresa X.

10.03.03 Firmas Digitales

1. Ejecución de Programa Java

Política: Los empleados no deben ejecutar aplicaciones Java descargadas de Internet a menos que la aplicación provenga de una fuente conocida y confiable, que se haya verificado la firma digital y que no se haya descubierto ningún problema.

Comentario: Este enfoque de ejecutar aplicaciones Java, también conocidas como applets, en computadores de escritorio tiene como intención prevenir que se ejecuten virus, caballos de Troya y demás códigos maliciosos en los computadores de la Empresa X. Esta política asume que los usuarios pueden distinguir entre

Comentario: Esta política informa a la comunidad de usuarios que no deben dejar archivos legibles en un protocolo de transferencia de archivos anónimos (FTP, por sus siglas en inglés), a menos que estos archivos hayan sido aprobados para su divulgación pública. Algunas organizaciones tienen empleados que han desarrollado el peligroso hábito de dejar archivos legibles en un servidor FTP anónimo de forma que los archivos pueden ser seleccionados por socios de negocios, clientes y otras personas externas a la organización. Esto expone estos archivos a acceso no autorizado por personas que se encuentren visitando el mismo servidor. Es relativamente fácil copiar una macro que borre periódicamente todos los archivos en el servidor web FTP anónimo que no se encuentran cifrados con un paquete interno de cifrado normal. Este es un proceso automático de refuerzo de esta política. Esta política también permite que una organización abandone la práctica de seguridad cuando personal dentro y fuera de la organización comparten el identificador del usuario y la contraseña fija, permitiéndose que personas externas tengan acceso a archivos que se encuentran en un servidor web. Otra razón deseable para cifrar estos archivos es que las modificaciones no autorizadas se harán evidentes de inmediato. Si el cifrado no se utiliza para este fin, pueden requerirse firmas digitales de forma que se detecten rápidamente los cambios no autorizados.

Políticas Relacionadas: “Transmisión de Datos Secretos”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

aquellas circunstancias en las que una firma digital ha sido verificada y no se ha presentado ningún mensaje de error al usuario, y aquellas circunstancias en las que el mecanismo de verificación de la firma digital se ha desactivado. La política asume una audiencia técnicamente alerta y una audiencia que se encuentra motivada por llevar a cabo esta tarea adicional. Para una audiencia menos sofisticada técnicamente, muchas organizaciones querrán simplemente bloquear el pasaje de entrada de programas con un cortafuego. El ámbito de esta política puede expandirse e incluir todo el contenido activo.

Políticas Relacionadas: “Inhabilitación de Java”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

2. Sitios Web y Comerciales en Internet

Política: Se requiere un certificado digital actualizado para todo servidor de Internet que maneje los negocios de la Empresa X y al que puedan conectarse clientes, prospectos y demás personas.

Comentario: Esta política evita que terceros establezcan sistemas en Internet que se disfrazan como sistemas de la Empresa X. Los certificados digitales son como pasaportes, porque definitivamente autentifican la identidad de los individuos o de los computadores. Los certificados digitales incluyen cierta información cifrada que permite que un tercero remoto verifique si

realmente ha llegado a un sistema genuino de la Empresa X. Esta utilización es relativamente poco costosa y provee uno de los mecanismos básicos de control necesarios para las actividades de comercio en Internet. La palabra "actualizado" es necesaria en la política debido a que las partes que autorizan los certificados los emiten por períodos breves de tiempo, lo que significa que necesitan ser renovados periódicamente.

Políticas Relacionadas: “[Autorización de Proceso de Cifrado — Usuarios](#),” “[Identificación Positiva para Uso del Sistema](#),” e “[Identificadores Personales en Ubicaciones Públicas](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10.03.04 Servicios de No Repudiación

1. Sistemas de Cifrado de Propósito General

Política: Todos los procesos de cifrado de propósito general que se ejecuten en los sistemas informáticos de la Empresa X deben incluir funciones de custodia de claves.

Comentario: Esta política requiere que los sistemas de cifrado utilizados para las actividades regulares de negocios empleen un sistema con custodia de claves. La custodia de claves permite que la gerencia u otras personas confiables, puedan evadir el proceso de cifrado cuando así lo requieran. Este proceso se requiere para proteger la clave especial que permite que se pueda romper el proceso de cifrado. Esto puede requerirse en caso de una emergencia, no disponibilidad del personal o investigaciones criminales. Sin las características de custodia de claves, la gerencia corre el riesgo de que el personal haga uso del poder que tiene de cifrar con propósitos maliciosos. Por ejemplo, el personal puede

utilizar el cifrado para encubrir actividades ilegales. La política no hace mención a los procesos de cifrado incrustados dentro de los sistemas informáticos. Se refiere a los sistemas de propósito general, no a los sistemas de cifrado de propósito especial como aquellos que manejan códigos para autenticación de mensajes, firmas digitales y cifrado de contraseñas. La política podría cambiarse para excluir el cifrado para sistemas de comunicación. La custodia de claves es necesaria para almacenar datos a través de paquetes de procesadores de palabras y programas utilitarios de cifrado independientes.

Políticas Relacionadas: “[Gestión Automática de Claves de Cifrado](#)” y “[Eliminación de Datos Fuente Después de Cifrar](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.03.05 Manejo de Claves

1. Divulgación de Claves de Cifrado — Autorización

Política: Las claves de cifrado no deben revelarse a consultores, contratistas, o terceros, a menos que se haya obtenido autorización del vicepresidente ejecutivo.

Comentario: Esta política informa a los trabajadores que las claves de cifrado deben protegerse con medidas de seguridad rigurosas. La gran mayoría de las tiendas de tecnología cifran las claves, si éstas se guardan en un archivo o en otro lugar donde pueden tener acceso personas no autorizadas. Esto significa que las claves de cifrado no se almacenan en la memoria principal de una máquina multiusuario, a menos que estén cifradas. Debe

utilizarse un mecanismo separado para el cifrado denominado "módulo de seguridad." La clave para la carga de los módulos y otros mecanismos debe utilizarse para prevenir que cualquier persona tenga acceso a la clave de cifrado.

Políticas Relacionadas: “[Sistemas de Gestión de Claves de Cifrado](#)” y “[Sospecha de Divulgación de Contraseña](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Sistemas de Gestión de Claves de Cifrado

Política: El sistema de cifrado de la Empresa X, debe diseñarse de manera tal que no sea una sola persona la que tenga el conocimiento completo de la clave de cifrado.

Comentario: Esta política evita que cualquier persona tenga acceso a la clave completa del cifrado. Si alguna persona posee una clave completa de cifrado, puede descifrar otras claves o información sensible valiéndose del sistema de instalación del cifrado. Esto puede llevar a fraude, sabotaje, invasión de la privacidad u otros problemas. Desglosando los componentes de las claves, tales actividades no son posibles sin que haya una trama. La separación de las claves en componentes generalmente involucra la creación de dos cadenas de bits, que al combinarse generan la producción de claves de cifrado. Con frecuencia, este proceso se automatiza a través del hardware. Las técnicas descritas en esta política pueden también aplicarse a contraseñas, inicialización de vectores, semillas generadoras de números seudo-aleatorios y otros parámetros utilizados en los procesos relacionados con seguridad.

Políticas Relacionadas: “[Separación de Tareas](#)” y “[Algoritmos Generadores de Contraseñas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

3. Delegación de la Responsabilidad en la Gestión

Política: La responsabilidad de la gestión de las claves debe delegarse solamente a personas que hayan pasado por una verificación de antecedentes, una auditoría de seguridad operacional, así como firmado un acuerdo de confidencialidad.

Comentario: Esta política impide que la gerencia media delegue la responsabilidad administrativa de las claves a organizaciones contratadas, servicios gubernamentales, socios de negocios, y otras organizaciones externas que no manejen claves en concordancia con las medidas de seguridad. Una política como ésta puede también utilizarse para nombrar al personal interno que se encargue de las obligaciones administrativas. La política describe un proceso para asegurar que la entidad receptora concuerde con los criterios de la Empresa X en lo relativo a personas confiables. Las organizaciones deben definir con precisión con quien compartirán la información sensible de la clave. Después, deben decidir cómo filtrar a las personas y las organizaciones, de modo que solamente las partes confiables reciban la información de la clave. Éste es el segundo paso que se refleja en esta política. Los tres criterios para determinar confiabilidad pueden modificarse para incluir otras consideraciones, como por ejemplo registrarse en una agencia gubernamental. Otra opción, puede ser asimismo, autoridades de certificación reconocidas como custodios de las claves para actividades comerciales en Internet. Los tres criterios mencionados en la política pueden clasificarse como de carácter personal y archivos históricos, prácticas operativas actuales y obligaciones legales. Esta política puede generalizarse e incluir otras responsabilidades de seguridad en una red de trabajo compartida, tal como la emisión del identificador de usuario y la administración de contraseñas.

Políticas Relacionadas: “[Otorgamiento de Privilegios del Sistema](#)” y “[Delegación de la Propiedad de la Información](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

4. Vigencia de los Certificados Digitales

Política: El período de validez para certificados digitales emitidos por la Empresa X no debe ser superior a un año.

Comentario: Esta política limita el daño que puede ocurrir si las claves privadas asociadas con un certificado digital cayeran en manos de una persona no autorizada y si la persona autorizada no informa a la autoridad de certificación (CA, por sus siglas en inglés). La CA es la organización de emisión, en este caso, la Empresa X. Un certificado digital es como un pasaporte para el uso de Internet, y estos certificados digitales formarán una parte crítica de la clave de la infraestructura pública futura. Limitando el certificado de vida a un

año, la continuidad de cualquier utilización no autorizada cesará. Mientras más corto sea el periodo de validez de un certificado digital, mayor será el nivel de seguridad. Lo mismo se aplica a las claves de cifrado. Mientras más frecuentemente se cambien, mayor será la seguridad del sistema asociado. El peligro de comprometer las claves privadas asociadas con un certificado digital disminuye por la existencia y distribución periódica de una lista de revocación de certificados (CRL, por sus siglas en inglés.) Una lista de revocación de certificados informará a los correspondientes que un certificado digital ya no tiene validez. La CA debe haber recibido un aviso de que el certificado ha sido comprometido, o supondrá que continúa válido. El registro en la Lista de Revocación de Certificados puede eliminarse después de que el certificado digital haya vencido. El tamaño de este listado se mantendrá dentro de los límites manejables, indicando el vencimiento automático del certificado digital.

Políticas Relacionadas: “[Segreto de la Clave de Cifrado](#)” y “[Ciclo de Vida de Claves de Cifrado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

5. Protección de Claves Raíces de Certificados Digitales

Política: La clave raíz para la jerarquía del certificado digital debe protegerse bajo seguridad física rigurosa, control dual, separación de componentes de clave y separación de tareas.

Comentario: Muchas organizaciones emiten sus propios certificados digitales. Debido a que varios procesos criptográficos, como por ejemplo las firmas y certificados digitales, dependen primordialmente de estas claves raíces, se hace imperativo que la clave raíz se guarde bajo la más estricta seguridad. Esta política tiene como objetivo enumerar cuatro (4) mecanismos específicos de seguridad, que deben emplearse en todos los casos. La seguridad física rigurosa significa, en líneas generales, el almacenamiento de información sensible en cajas fuertes, que requiera de identificación o lector de distintivos para permitir el acceso físico al equipo, o mantener el registro de quienes tienen acceso al equipo mediante la utilización de circuito cerrado de televisión. El control dual se refiere al uso de no menos de dos personas para llevar a cabo procedimientos tales como la generación de la clave raíz. Los componentes divididos de las claves son el resultado de transformaciones matemáticas que ocultan claves. La separación

de las tareas, se refiere al uso de personas diferentes para realizar actividades diferentes, ya que cada uno verifica el trabajo del otro.

Políticas Relacionadas: “[Delegación de la Responsabilidad en la Gestión](#)” y “[Sitios Web y Comerciales en Internet](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

6. Transmisión de Datos y Claves de Cifrado

Política: Si se utilizan los cifrados y si las claves se transmiten en forma legible a otra persona, la información protegida con cifrado debe transmitirse a través de un canal de comunicación diferente al de las claves utilizadas para manejar el proceso de cifrado.

Comentario: Esta política evita que un interceptor de líneas tenga acceso a versiones legibles de tanto las claves como los datos sensibles. Si la persona que intercepta descifra el proceso de cifrado, entonces tendrá toda la información necesaria para romper nuevas transmisiones. El proceso de enviar claves a través de un canal de comunicación separado aumenta su nivel de esfuerzo. Un ejemplo sería remitir las claves por correo y no a través de la red del computador que une los grupos de comunicación. Esta política acepta la utilización de un algoritmo tradicional de cifrado simétrico, en donde la clave de cifrado es la misma que la clave de descifrado. Esta política no es necesaria si se utilizan algoritmos asimétricos donde la clave de cifrado sea diferente a la clave de descifrado. Los protocolos de manejo de claves en Internet utilizan el último de los dos tipos de algoritmos mencionados. Esta política no es necesaria si solamente se utilizan protocolos normales de Internet.

Políticas Relacionadas: “[Separación de Tareas](#),” “[Medios de Almacenamiento de Claves de Cifrado](#),” y “[Sistemas de Gestión de Claves de Cifrado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

7. Gestión Automática de Claves de Cifrado

Política: Si están disponibles comercialmente, la Empresa X debe emplear procesos automatizados de gestión de claves.

Comentario: Esta política ahorra dinero y tiempo a la Empresa X, y obtiene el sistema de seguridad más efectivo disponible. Para algunos sistemas de cifrado, no hay procedimientos comercialmente disponibles aplicables a la gestión de claves. Sin embargo, ofertas comerciales recientes incluyen varios sistemas poderosos de gestión de claves. La automatización reduce la probabilidad de que accidentalmente se divulgue una clave a personas no autorizadas. Algunas organizaciones prefieren colocar la palabra "normal" dentro de la política para asegurar interoperatividad con otros sistemas de gestión de claves.

Políticas Relacionadas: “Responsabilidad de la Gestión de Claves” y “Sistemas de Gestión de Claves de Cifrado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

8. Ciclo de Vida de Claves de Cifrado

Política: Las claves utilizadas para el cifrado de datos de la Empresa X deben cambiarse por lo menos cada noventa (90) días.

Comentario: Esta política requiere de cambios periódicos en las claves de cifrado. El cambio de las claves aumentará la seguridad del sistema de cifrado. Si el adversario es capaz de obtener una clave de cifrado en particular a través del análisis, tendrá que comenzar desde el principio, cuando se cambie la clave. Debido a que se preocupan por la solidez de la longitud limitada de las claves de algunos algoritmos, algunas organizaciones requieren que las claves se cambien en cada transmisión. Otra opción es utilizar cifrado triple, un proceso que emplea dos claves para un solo proceso de cifrado. Para aumentar más aún el nivel de esfuerzo requerido por los adversarios, algunas organizaciones querrán cambiar los vectores de inicialización periódicamente.

Políticas Relacionadas: “Vencimiento de Claves de Cifrado” y “Cambios Obligatorios de Contraseña”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

9. Vencimiento de Claves de Cifrado

Política: Todas las claves de cifrado deben tener un tiempo de vida establecido y deben cambiarse durante o antes de la fecha de vencimiento.

Comentario: Esta política establece que las personas que manejen claves deben asignarles una fecha de vencimiento a dicha clave. No debe aceptarse la utilización de claves que no tengan fecha de vencimiento a menos que se utilice un cifrado en bloque válido por una sola vez. Los cifrados válidos por una sola vez son ineficientes, costosos y pocas veces se utilizan fuera de los círculos militares o diplomáticos. Como estas claves sólo se pueden usar una vez, no necesitan ni fecha de vencimiento ni del establecimiento de un período de vida. Todos los demás sistemas utilizan la misma clave reiteradamente. Después de un tiempo, la seguridad que suministran estos otros sistemas de cifrado se degradan. Es necesario cambiar la clave para reforzar la seguridad del proceso de cifrado. Un sistema de cifrado donde cada sesión o transacción tiene su propia clave, suministrará una seguridad mayor, cosa que no sucede cuando se utiliza la misma clave durante varios meses. Desde el punto de vista conceptual, el tiempo de vida establecido para una clave de cifrado se relaciona y es similar a las etiquetas de clasificación de sensibilidad utilizadas para datos comunes.

Políticas Relacionadas: “Ciclo de Vida de Claves de Cifrado” y “Etiquetado Durante el Ciclo de Vida de la Información”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10. Generación de Claves de Cifrado

Política: Cuando se utilice el cifrado, las claves deben ser generadas a través de medios poco discernibles para el adversario, y que originen claves difíciles de adivinar.

Comentario: La intención de este proceso es cerciorarse que los sistemas de cifrado suministren toda la seguridad que es capaz de proporcionar. Si las claves de cifrado se adivinan fácilmente, la seguridad suministrada por los sistemas de cifrado puede también comprometerse fácilmente. Por ejemplo, si los usuarios escogen sus propias claves de cifrado, se recomienda un filtro para protegerla contra suposiciones. Esta política se deriva de otra relacionada con claves no rigurosas. Algunas claves no rigurosas hacen el análisis DES más fácil, por lo que deben evitarse. Con frecuencia el proceso de generar claves es parte de un proceso automatizado de gestión de claves, en cuyo caso esta política no será necesaria.

Políticas Relacionadas: “Gestión Automática de Claves de Cifrado,” “Longitud de Claves de Cifrado Seleccionadas por Usuarios,” y “Semilla para Contraseñas Generadas por el Sistema”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

11. Longitud de Claves de Cifrado Seleccionadas por Usuarios

Política: Cuando el usuario elige las claves de cifrado, el sistema de cifrado debe impedir al usuario crear claves con menos de diez (10) caracteres.

Comentario: Esta política garantiza que el sistema de cifrado suministrará la seguridad que se supone debe suministrar. Si las claves de cifrado se adivinan fácilmente, el sistema de cifrado caerá en riesgos con facilidad. Los 10 caracteres no significan nada especial, pero para ambientes con un nivel de seguridad muy alto el número puede ser mayor, mientras que para ambientes bajos y medios, el número puede ser un poco menor. Deben garantizarse otros mecanismos de filtro para la utilización de claves de cifrado seleccionadas por el usuario. Por ejemplo, algunos algoritmos tienen muchas claves débiles que permiten que el proceso de cifrado se derrote fácilmente. Estas claves débiles no se deben permitir.

Políticas Relacionadas: “Generación de Claves de Cifrado” y “Longitud Mínima de Contraseñas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

12. Materiales para la Generación de Claves

Política: Cuando se utilice el cifrado, los materiales para desarrollar las claves de cifrado y las copias impresas de versiones de claves deben mantenerse todas en un lugar seguro y bajo llave.

Comentario: Los materiales para la generación de claves incluyen los datos de las claves de cifrado, claves que cifren otras claves, también llamadas claves maestras, inicialización de vectores, semillas generadoras de números seudo-aleatorios y otros parámetros utilizados para controlar o iniciar procesos de cifrado. Esta política evita que los parámetros utilizados para la construcción de claves de cifrado lleguen a manos equivocadas y sean utilizadas para construir claves de cifrado o inteligentemente adivinar las claves de cifrado.

Después de utilizado, este material para las claves debe destruirse tan pronto como sea posible de acuerdo con los procedimientos autorizados para información secreta. La utilidad de esta política puede parcialmente superarse a través de la utilización de sistemas automatizados de gestión de claves.

Políticas Relacionadas: “Destrucción de Materiales para Generación de Claves” y “Gestión Automática de Claves de Cifrado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

13. Claves Maestras de Cifrado en Texto

Política: Las claves maestras en texto deben manejarse manualmente a través de un control dual con conocimiento separado o almacenarse en módulos a prueba de todo.

Comentario: Esta política especifica las maneras permitidas de proteger el tipo de cifrado de mayor sensibilidad. Las claves maestras se utilizan para el cifrado de todas las demás claves, o al menos para el cifrado de claves que cifren otras claves. Si se revela una clave maestra, el sistema completo de cifrado puede comprometerse rápidamente. Se necesitan mayores esfuerzos para prevenir que estas claves caigan en manos equivocadas. Cuando las claves maestras estén diseñadas para que se puedan leer, deben ser segmentadas. Cada componente no revelará la clave maestra original. Pueden guardarse en módulos de hardware que automáticamente borren las claves si alguien altera el módulo. A estos módulos generalmente se les llaman “módulos de seguridad”.

Políticas Relacionadas: “Materiales para la Generación de Claves” y “Sistemas de Gestión de Claves de Cifrado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

14. Destrucción de Materiales para Generación de Claves

Política: Todos los materiales utilizados para generar, distribuir y almacenar claves deben protegerse y no divulgarse a personas no autorizadas. Cuando estos suministros ya no sean necesarios, deben destruirse mediante el uso de máquinas trituradoras de papeles, incineradores u otros métodos autorizados.

Comentario: Esta política evita que personas no autorizadas obtengan acceso a información utilizada para generar, distribuir o almacenar claves de cifrado, lo cual incluye copias al carbón y cintas de impresión. Esto podría permitir que las partes consigan copias de las claves, y así apoderarse de información sensible protegida por el cifrado. Esta política alerta a los trabajadores que estos materiales son sensibles y deben manejarse con cuidado.

Políticas Relacionadas: “[Materiales para la Generación de Claves](#),” “[Disposición de Información en Papel](#),” y “[Materiales Usados con Información Sensible](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

15. Destrucción de Material de Intercambio de Claves

Política: Los custodios del material de intercambio de claves deben destruir este material de acuerdo con los procedimientos autorizados, dentro de un período razonable que no exceda los diez (10) días hábiles siguientes a la verificación comprobada del proceso de intercambio de claves.

Comentario: La intención de esta política es la de especificar claramente cuándo los Custodios deben destruir los materiales correspondientes a las claves que han recibido. Mientras menos tiempo estén los materiales fuera del sistema y menos cantidad de personas tengan acceso, más seguro estará el proceso de cifrado. Los ambientes de red multiorganizacionales tienen la necesidad específica de esta política, pues mientras el proceso de automatización de la administración de claves va en aumento, existen muchos sistemas de cifrado donde se requiere la carga manual de claves y otro tipo de tecnología, y por ello hace falta la intervención del ser humano; razón por la cual se creó esta política de procedimientos manuales.

Políticas Relacionadas: “[Productos Intermedios Con Información Sensible](#)” y “[Materiales Usados con Información Sensible](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

16. Secreto de la Clave de Cifrado

Política: La privacidad de cualquier clave de cifrado que se utilice por confidencialidad debe mantenerse intacta mientras toda la información protegida se considere confidencial.

Comentario: Esta política le proporciona a los diseñadores y operadores de sistemas el principio básico de seguridad para los sistemas de gestión de claves. La política advierte que no deben divulgarse las claves de cifrado mientras se considere confidencial toda la información protegida con estas claves. Desde el punto de vista práctico, y en muchos casos, este período será más largo que el tiempo de vida de una persona. La privacidad de la clave se mantiene asegurada si ha sido destruida a través de un proceso autorizado. Por ejemplo, si se han enviado datos confidenciales por Internet en forma cifrada, la clave podría destruirse aunque la información sea confidencial. Esta política enfatiza la importancia de la privacidad de las claves, un mensaje a veces desconocido o ignorado por los usuarios del sistema de cifrado. La vida de una clave se mantiene mientras dure el período de uso.

Políticas Relacionadas: “[Ciclo de Vida de Claves de Cifrado](#)” y “[Vencimiento de Claves de Cifrado](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Medianos y altos

17. Ciclo de Vida de las Claves Privadas de Firmas Digitales

Política: Las claves privadas de las firmas digitales deben mantenerse confidenciales al menos por el número de años que puedan utilizarse en materia legal.

Comentario: Esta política informa a los usuarios el tiempo que deben mantener sus claves privadas utilizadas para firmas digitales. El número exacto de años variará de acuerdo con la jurisdicción, y por este motivo no aparece establecido en la política. Para una empresa multinacional, esta política puede ir acompañada de un cuadro donde se demuestren los requerimientos de diferentes países, o el número máximo de años que pueden colocarse dentro de la política misma. La política puede extenderse para incluir la necesidad de una medida de integridad de datos, como una suma de verificación para asegurar que la clave de la firma digital no ha sido corrompida. Algunas empresas querrán destruir las claves privadas al no poderlas utilizar por más tiempo y después apoyarse en claves públicas para probar la autenticidad de un mensaje. Esto es posible con el sistema de claves

públicas localizadas en Internet donde las claves privadas difieren de las públicas. Por otra parte, aquellas organizaciones que desean mantener las claves privadas para asuntos legales, utilizarán esta política. Esta política puede aplicarse a cualquier tipo de organización que utilice sistemas tradicionales de cifrado de claves simétricas. Las firmas digitales son procesos especiales de cifrado que prueban que un grupo específico generó un mensaje y que personas no autorizadas no lo han modificado. Las claves privadas de firmas digitales deben mantenerse en secreto, mientras que las claves públicas de firmas digitales están completamente disponibles y generalmente no se mantienen en secreto.

Políticas Relacionadas: “Claves de Firmas Digitales y de Autentificación de Usuarios” y “Ejecución de Programa Java”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Respaldos de Claves Privadas

Política: Los usuarios no deben permitir que los sistemas automáticos de respaldo hagan copias de la versión legible de su clave privada utilizada para firmas digitales y certificados digitales.

Comentario: Esta política mantiene la confidencialidad de las claves de cifrado privadas que se utilizan tanto para firmas digitales como para certificados digitales. Estas claves privadas las debe guardar bajo su control el usuario a quien pertenezcan. Si los usuarios simplemente almacenan la versión legible de sus claves privadas en el disco duro de un computador personal, los sistemas de respaldo automático pueden transferir estas claves privadas a los medios de almacenamiento de respaldo donde las partes no autorizadas pueden encontrarlas. Esta política no evita que el usuario haga un respaldo en disco y lo guarde en una caja de seguridad.

Políticas Relacionadas: “Claves de Firmas Digitales y de Autentificación de Usuarios” y “Protección de Claves Raíces de Certificados Digitales”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Duplicación de Claves de Cifrado

Política: Las claves de cifrado utilizadas para ocultar datos respaldados también deben respaldarse y almacenarse bajo medidas de seguridad tan rigurosas o más que las aplicadas al respaldo de los datos pertinentes.

Comentario: Esta política garantiza que el personal del sistema de información ha tomado las medidas necesarias para respaldar con medidas de seguridad las claves de cifrado que se utilizan para proteger los medios de respaldo. Si no se han respaldado adecuadamente las claves, los esfuerzos para recobrar los datos pueden obstaculizarse severamente o hasta impedirse. Las instituciones financieras, oficinas de crédito, laboratorios de investigación y otras organizaciones que almacenan respaldos en otras localidades, emplean generalmente el cifrado de sus medios de respaldo. Esta política indica que las claves deben protegerse tanto como los propios datos. Esto se debe a que la seguridad física en otra localidad puede comprometerse fácilmente, en cuyo caso el proceso de cifrado es el único control de seguridad que previene la divulgación de los datos respaldados.

Políticas Relacionadas: “Claves de Firmas Digitales y de Autentificación de Usuarios” y “Medios de Almacenamiento de Claves de Cifrado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

20. Divulgación de Claves de Cifrado — Controles

Política: Las claves de cifrado deben protegerse de la divulgación no autorizada a través de controles técnicos, tales como cifrados en claves separadas y la utilización de un hardware resistente a modificaciones.

Comentario: Esta política establece que deben tomarse medidas para evitar la divulgación no autorizada de las claves de cifrado. Si estas claves se divultan, se destruirá en muchos casos la seguridad de los sistemas de cifrado. El hardware resistente evita que la gente abra los mecanismos de cifrado y recuperen las claves de cifrado allí almacenadas. En los llamados “módulos de seguridad”, este hardware borra automáticamente las claves allí contenidas en caso de que el módulo sea abierto. Este hardware también está protegido para que las emanaciones electromagnéticas no revelen las claves almacenadas. En términos de usar el cifrado para cifrar claves, en vez de utilizar sólo una clave maestra para cifrar otras claves, muchas organizaciones utilizan una jerarquía de claves maestras. Esto puede complicarse y presentarnos otra razón por la cual es importante automatizar el proceso de gestión de claves.

Políticas Relacionadas: “Gestión Automática de Claves de Cifrado” y “Módulos de Hardware para el Proceso de Cifrado”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

21. Seguridad de Clave Privada para Certificados Digitales

Política: La clave privada asociada a cada trabajador en la Empresa X debe protegerse para que no sea divulgada sin autorización cuando no esté en uso, aplicando técnicas más avanzadas en lugar de una simple medida física de seguridad.

Comentario: Esta política informa a los usuarios que deben proteger sus claves privadas contra cualquier divulgación o utilización fraudulenta. Si se descubre una clave sin proteger, puede ser utilizada sin autorización. Así como al tarjetahabiente se le advierte no dejar sus tarjetas de crédito desatendidas, esta política informa que los que posean una clave deben tomar ciertas precauciones a fin de mantener la seguridad de los procesos de cifrado que dependen de sus claves privadas.

Políticas Relacionadas:“[Ciclo de Vida de las Claves Privadas de Firmas Digitales](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

22. Almacenamiento de Claves de Cifrado y Firmas Digitales

Política: Las claves empleadas por los usuarios finales para cifrar y para las firmas digitales deben ser almacenadas en dispositivos con hardware resistente a modificaciones.

Comentario: Esta política impide que personas no autorizadas tengan acceso a las claves de cifrado o claves de firma digital. Si estas personas lograron el acceso, igualmente pueden lograr examinar información confidencial prohibida para ellos, hacerse pasar por otros e iniciar transacciones que no estén autorizados a iniciar. El almacenamiento en una tarjeta inteligente se acepta como el modo más seguro de proceder, pero es más costoso y complejo de administrar. Tal vez el aspecto más problemático acerca de la utilización de las tarjetas inteligentes es la instalación de lectores en los computadores personales. Encontrar personal con suficiente experiencia para instalar y administrar sistemas de tarjetas inteligentes es difícil. Se puede utilizar un número de identificación personal o contraseña establecida para activar el uso de las tarjetas

inteligentes. Esto significa que alguien que robe una tarjeta inteligente, o que encuentre una tarjeta inteligente perdida, no puede utilizarla para fines no autorizados. Si estas claves se almacenan en el escritorio del computador, los usuarios deben asegurarse de cifrarlas con contraseñas sólidas.

Políticas Relacionadas:“[Módulos de Hardware para el Proceso de Cifrado](#)” e “[Información Sensible en Computadores Personales](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

23. Transmisión de Claves de Cifrado Privadas

Política: Si las claves de cifrado privadas se transmiten a través de líneas de comunicación, deben estar cifradas con un algoritmo más poderoso que el utilizado para cifrar otros datos secretos protegidos por dicho cifrado.

Comentario: Esta política evita que los usuarios envíen inadvertidamente claves de cifrado privadas legibles a través de sistemas de comunicación. Si lo hacen, el proceso de cifrado puede ser burlado con facilidad. Esta política se aplica tanto a los nuevos sistemas de claves de cifrado como a los sistemas de cifrado simétricos tradicionales. Cualquiera que sea la tecnología utilizada, las claves privadas nunca deben enviarse sin cifrar.

Políticas Relacionadas:“[Transmisión de Datos y Claves de Cifrado](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

24. Cambios en Claves Públicas

Política: Si una clave de cifrado pública ha sido publicada en un servidor web o en otro sitio de acceso público, se debe notificar a todos los correspondientes regulares cada vez que haya cambios en dicha clave pública.

Comentario: Esta política es importante solamente para aquellas organizaciones que utilizan sistemas de cifrado con claves públicas. Esta política reconoce que algunos sistemas de cifrado permiten al usuario colocar su clave pública en un lugar público. Esto permite que el correo electrónico y otras transmisiones sean fácilmente cifradas, y también permite la fácil revisión de firmas digitales. Con este enfoque existe la posibilidad de que un impostor pueda hacerse pasar por un usuario original.

Hasta que ocurra su detección, este impostor puede engañar a los correspondientes para que se comuniquen con él en vez de hacerlo con el usuario original. Esta política previene ese abuso o al menos reduce significativamente el tiempo en el que pueda ocurrir. Los mensajes que notifican a los correspondientes de futuros cambios a una clave pública pueden firmarse con una clave privada que aún no haya vencido. Esto le asegura a los correspondientes que han recibido un mensaje del usuario legítimo y no de un impostor.

Políticas Relacionadas:“[Transmisión de Claves de Cifrado Privadas](#)”

Política Dirigida a:Todos

Ambientes de Seguridad:Medianos y altos

25. Claves Comprometidas

Política: Las claves de cifrado que se han comprometido, o revelado a terceras personas de conformidad con un acuerdo de custodia de clave, deben revocarse inmediatamente, en forma retroactiva al último momento conocido en que las claves estaban a salvo.

Comentario:Esta política apoya la flexibilidad de recuperación de los sistemas de gestión de claves. Esta política sustenta la rápida notificación a otros participantes en el sistema de administración de claves, y después, la pronta emisión de nuevas claves confiables. Si las claves reveladas a terceros fuesen revocadas sólo hasta el punto en que se supo que ocurrió la divulgación, entonces pudieron haber existido compromisos previos y no percibidos hasta entonces por el portador de la clave o de la autoridad que la haya manejado. Si se continúa el soporte de transacciones y mensajes ejecutados y enviados a donde pudiesen haber existido claves comprometidas y no divulgadas, es posible que exista allí un fraude encubierto. La clave comprometida se revoca entonces de regreso al punto donde estaba protegida. Este punto generalmente coincide con un cambio previo de clave.

Políticas Relacionadas:“[Sistemas de Cifrado de Propósito General](#)” y “[Contraseñas y Claves en Utilidades de Cifrado](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

26. Medios de Almacenamiento de Claves de Cifrado

Política: Si se utiliza el cifrado para proteger datos sensibles residentes en los medios de almacenamiento de un computador, la clave de cifrado y los materiales de cifrado de claves correspondientes utilizados en el proceso de cifrado, no deben guardarse en ninguno de los medios de almacenamiento mencionados sin su correspondiente cifrado.

Comentario:Esta política evita que el analista se aproveche del hecho de que los materiales de cifrado de claves están almacenados en el mismo medio en que se almacenan los datos cifrados. Si estos materiales se almacenan juntos, entonces es factible que el proceso asociado con el cifrado resulte inoperante. Muchos de los paquetes comerciales de cifrado utilizan este enfoque. No es aceptable la utilización de archivos o directorios ocultos para el almacenamiento no cifrado de estos materiales de cifrado.

Políticas Relacionadas:“[Transmisión de Datos y Claves de Cifrado](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

27. Controles en la Operación de Recuperación de Claves

Política: Cada vez que se recuperen claves del archivo de claves de cifrado deben estar presentes dos funcionarios autorizados del personal de la Empresa X, y todas estas operaciones deben ser registradas de manera segura.

Comentario:Esta política evita que sea un solo integrante del personal el que utilice el sistema de recuperación de claves. Si es una sola persona quien recupera las claves, puede hacerse pasar por otra y utilizar las firmas digitales, además examinar archivos confidenciales que no tenga autorización para ver. Esta política requiere un control dual, lo que indica que para obtener un nivel más alto de seguridad, tienen que estar dos personas confiables presentes antes de realizarse una operación sensible.

Políticas Relacionadas:“[Contraseñas y Claves en Utilidades de Cifrado](#)” y “[Sistemas de Cifrado de Propósito General](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Medianos y altos

28. Claves de Cifrado de Respaldo

Política: Si el trabajador de la Empresa X va a emplear cifrado en las actividades de procesamiento de la información del negocio de producción, este trabajador debe entregar de manera segura copias de respaldo de todas las claves a la gerencia del departamento de Seguridad Informática.

Comentario: Esta política compensa las deficiencias de muchos de los paquetes de software de cifrado. La política le permite a la organización disfrutar de los beneficios de un custodio garantizado de claves, aunque el paquete de cifrado que estén utilizando no incluya funcionalidad de custodia garantizada de claves. El propósito de la custodia garantizada es poder leer los datos protegidos aun cuando la clave de cifrado pertinente haya sido extraviada o robada. Los mecanismos de custodia garantizada de claves pueden emplear una clave separada que permita descifrar los datos cifrados, aun cuando no esté disponible la clave de cifrado original. De conformidad con esta política, se entregan copias de respaldo de las claves de cifrado a un tercero de confianza, en este caso un especialista en seguridad informática de la misma empresa. Algunos usuarios pueden considerar esta política como una injerencia, pero no lo es, ya que se refiere solamente a la información de producción y no a detalles personales.

Políticas Relacionadas: “[Llaves de las Estaciones de Trabajo](#)” y “[Contraseñas y Claves en Utilidades de Cifrado](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

29. Claves de Firmas Digitales y de Autentificación de Usuarios

Política: Las claves que se utilicen para firmas digitales, certificados digitales, y autentificación de usuarios nunca deben incluirse en un acuerdo de custodia garantizada de claves.

Comentario: Esta política se utiliza para garantizar que los usuarios no puedan rechazar o repudiar voluntariamente sus claves de cifrado, proceso también conocido como de no repudiación. La repudiación causaría caos respecto de los procedimientos legales que dependen de firmas digitales u otros mecanismos de seguridad fundamentados en claves de cifrado. En general, las firmas digitales y varias otras medidas de control suponen que sólo el usuario respectivo tiene control sobre la clave o la contraseña. Pero la custodia garantizada de claves es un acuerdo mediante el cual las claves de cifrado pueden ser compartidas con algunas organizaciones.

Políticas Relacionadas: “[Sistemas de Cifrado de Propósito General](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

30. Separación de Claves de Cifrado y de Firmas Digitales

Política: Si se utilizan tanto la firma digital como el cifrado, deben utilizarse claves separadas en cada una de estas dos medidas de control.

Comentario: Esta política evita que un adversario que tome posesión de una clave, comprometa tanto el cifrado como los sistemas de firmas digitales. Si se utilizan claves separadas, el esfuerzo requerido para vencer un sistema es mayor, suponiendo que tanto las firmas digitales como el cifrado deben estar comprometidos para poder comprometer todo el sistema. Con claves separadas, tanto la complejidad como el costo de los sistemas de seguridad también aumentan. Las firmas digitales son pequeños anexos que se agregan a los mensajes o archivos para reflejar que se les ha aplicado un proceso de cifrado, y se utilizan para mostrar que los mensajes o archivos provienen de fuentes autorizadas y que no han sido alterados. Se les conoce también como códigos de autentificación de mensajes.

Políticas Relacionadas: “[Medios de Almacenamiento de Claves de Cifrado](#)” y “[Transmisión de Datos y Claves de Cifrado](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

31. Responsabilidad de la Gestión de Claves

Política: Cuando se utilice el cifrado para proteger datos sensibles, el Propietario respectivo de los datos debe asignar explícitamente la responsabilidad del manejo de la clave de cifrado.

Comentario: Cuando se utiliza el cifrado, la responsabilidad de proteger los datos sensibles se cambia a responsabilidad de proteger claves de cifrado. La actividad de protección es necesaria, aunque la cantidad de información que necesita protegerse disminuya dramáticamente. Es importante lograr que los propietarios de los datos pertinentes asignen la respon-

sabilidad que corresponde a la gestión de la clave. Esta política obliga a los Propietarios a explícitamente realizar tal asignación. La política supone que el cifrado se maneja de manera descentralizada en las organizaciones, en lugar de manera centralizada por la gerencia de Tecnología Informática o por la de Seguridad Informática.

10.04 Seguridad de los Archivos del Sistema

10.04.01 Control del Software de Operaciones

1. Prueba del Sistema de Aplicaciones de Negocios

Política: Todos los sistemas de aplicación desarrollados internamente deben pasar por tres ciclos de pruebas donde se descubran y corrijan todos los errores antes de poner los sistemas de aplicación en operación de producción.

Comentario: Esta política garantiza que los sistemas de aplicación de negocios en producción serán confiables y estarán razonablemente libres de errores graves de codificación, otros errores serios, características distintas a las especificaciones y otros problemas. El enfoque tradicional relativo al desarrollo de sistemas exige un ciclo de pruebas, esfuerzos para resolver los problemas y una prueba de regresión, para luego realizar el lanzamiento de la aplicación en producción. El problema con este enfoque tradicional es que las correcciones de errores y los otros cambios que se hagan después del ciclo de pruebas incorporan nuevos errores y otros problemas. Estos nuevos errores y problemas pueden no ser descubiertos en la prueba de regresión, y el cronograma no permitía su resolución. Esta política adopta un enfoque más riguroso, que reemplaza el largo ciclo inicial de pruebas al final del proceso de desarrollo con tres ciclos más cortos. Esta política generalmente aumenta el tiempo y dinero requeridos para desarrollar una aplicación, pero asimismo bajará los costos a largo plazo.

Políticas Relacionadas: “Acceso del Desarrollador a la Información de Producción” y “Convenciones en Desarrollo de Sistemas”

Políticas Relacionadas: “Propiedad de la Información” y “Gestión Automática de Claves de Cifrado”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Migración de Software

Política: El personal de desarrollo de sistemas y aplicaciones no debe tener facultad para trasladar ningún software al ambiente de producción.

Comentario: La función de esta política es prevenir que los desarrolladores trasladen anticipadamente sus propios sistemas a producción. Lo pueden hacer por ejemplo para evitar pruebas completas que revelen medidas de control inadecuadas. También puede que quieran movilizar sus propios sistemas a producción apresuradamente para evitar otras revisiones que revelen códigos no autorizados. El objetivo descrito en esta política puede ser difícil de lograr, si hay pocas personas en una organización, o si los computadores personales o estaciones de trabajo tienen que manejar las versiones de producción de estas aplicaciones. Muy poco personal requerirá un balance en términos de la separación de las tareas; además, el uso de sistemas pequeños como sistemas cliente-servidor o redes de área local frecuentemente previene la separación rigurosa de desarrollo y producción.

Políticas Relacionadas: “Separación de Tareas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.04.02 Protección de los Datos de Prueba del Sistema

1. Información Usada en Pruebas de Software

Política: A menos que se obtenga un permiso por escrito de la gerencia de Seguridad Informática, toda prueba de software de sistemas diseñada para manejar información privada debe llevarse a cabo con información de producción que no contenga detalles específicos que puedan ser valiosos, críticos, confidenciales ni privados.

Comentario: Por ejemplo, un proceso de desinfección de información puede ocultar cierta información sin modificar las características particulares de la prueba. Digamos, por ejemplo, los nombres y apellidos de las personas que aparecen en una base de datos de Recursos Humanos puede mezclarse de tal manera que ya no reflejen a ninguna persona en particular. De esta manera la longitud requerida para los campos, el número de registros en la base de datos y otras estadísticas permanecen igual para propósitos de pruebas. Esta política previene que personas como programadores y contratistas de la Empresa divulguen información no autorizada de la información de prueba. Esta política se ajusta a los paquetes para terceras personas y software desarrollado en casa. Además, es particularmente importante para aquellos ambientes en los cuales los usuarios finales elaboran sus propios programas. Muchas organizaciones querrán definir el proceso de limpiar los datos. En vez de mencionar información valiosa, crítica, confidencial o privada, esta política permite la referencia a ciertas clasificaciones de datos utilizadas dentro de la Empresa X.

Políticas Relacionadas: ‘‘Clasificación de Datos en Cuatro Categorías,’’ ‘‘Divulgación de Información Privada a Terceros,’’ y ‘‘Acceso del Desarrollador a la Información de Producción’’

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

2. Acceso del Desarrollador a la Información de Producción

Política: Cuando se requiera el acceso a la información de negocios de producción para desarrollar o probar sistemas de aplicaciones nuevas o modificadas, sólo debe concederse acceso a la ‘‘lectura’’ o ‘‘copia’’ de datos en las máquinas de producción mientras duren las pruebas y trabajos del desarrollo pertinente, y deben desautorizarse tan pronto haya finalizado con éxito el trabajo.

Comentario: Esta política indica el momento en el cual se concederá acceso a los datos de negocio de producción residentes en las máquinas de producción al personal de pruebas, como por ejemplo a los expertos en aseguramiento de la calidad. La política limita estrictamente el tipo de acceso que tendrán. Después de leer y copiar de nuevo los datos de producción en un sistema de prueba, pueden actualizarlos y borrarlos según sea necesario en la máquina de prueba. La política enfatiza una clara distinción entre ambientes de producción y de desarrollo. La política también indica el tipo de derechos de acceso que se otorgará a los desarrolladores. Asimismo, define derechos de acceso a un área donde el exceso de derechos en algunas ocasiones es muy común. Sin una política como ésta y medidas de control relacionada, será difícil establecer una clara separación entre los ambientes de producción y desarrollo de computación. La política también previene e impide la manipulación de los datos de producción por parte del desarrollador. También supone que los usuarios de producción son personas diferentes de los que hacen el desarrollo y las pruebas. Aunque no se encuentran específicamente aludidos por esta política, el personal de desarrollo debe ser diferente del personal de pruebas.

Políticas Relacionadas: ‘‘Restricción de Privilegios — Necesidad de Conocer,’’ ‘‘Acceso a la Información de las Aplicaciones de Producción,’’ e ‘‘Información Usada en Pruebas de Software’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.04.03 Control de Acceso a la Biblioteca Fuente de Programas

1. Privilegios del Personal Técnico

Política: El personal de operaciones de computación no debe tener acceso a los datos de producción, programas de producción o sistemas operativos más allá de lo necesario para desempeñar su trabajo.

Comentario: Esta política es un ejemplo específico de separación de tareas, tal como que se refleja en un centro de datos que utilice una máquina mainframe. Debido a que los mecanismos de control de acceso pueden no estar disponibles para la separación adecuada de tareas, esta política puede no resultar práctica para sistemas menores como computadores personales o estaciones de trabajo. A medida que Internet permita la existencia de extranets y otras sociedades de negocios, la política se hará más aplicable al ambiente de sistemas pequeños. La intención de esta política es la de indicar claramente que el personal de operaciones de computación no debe recibir acceso universal a los datos de producción, a los programas de producción y al sistema operativo. Dado que este control se ignora a menudo en los centros de procesamiento de datos, se requiere una política específica para aclarar cuál será el procedimiento exacto a seguir.

Políticas Relacionadas: “[Restricción de Privilegios — Necesidad de Conocer](#)” y “[Separación de Tareas](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Acceso a Programas e Información de Producción

Política: Los controles de acceso se deben configurar de tal manera que no se concedan al personal de soporte técnico de software de sistemas informáticos y programas de producción, derechos de acceso sino para

resolver problemas, que no se le concedan derechos para actualizar los sistemas de software al personal de desarrollo de aplicaciones, como tampoco el acceso a la copia maestra de la información de producción excepto para resolver problemas, y que prohíban que el personal de operaciones de computación modifique el software de sistemas, el software de las aplicaciones y la información de producción.

Comentario: Esta política define la clásica y tan frecuentemente nombrada separación de tareas entre el personal que trabaja en las áreas de operaciones de computación, soporte de software de sistemas y desarrollo de aplicaciones. La intención de esta política es prevenir que la gente que trabaja en una de estas tres áreas abuse de sus derechos, y cause daños a los programas o a la información. Hay dos excepciones en esta política que permiten el acceso, que normalmente estaría prohibido, con el fin de resolver problemas serios. En estas circunstancias, es recomendable extender los registros para que luego el supervisor o administrador revise el trabajo de los que recibieron derechos adicionales. Esta política no se puede implementar a menos que se haya instalado un control de acceso en los sistemas computarizados de producción de las organizaciones que adopten esta política. Estos sistemas de control de acceso generalmente no se encuentran en computadores personales, sino en grandes sistemas multiusuario. Esta política no cubre un proceso de control de cambios para el desarrollo, prueba y traslado a producción de los programas de aplicación.

Políticas Relacionadas: “[Acceso a Comandos del Sistema Operativo](#)” y “[Privilegios Sobre la Información de Producción](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10.05 Seguridad en los Procesos de Desarrollo y Soporte

10.05.01 Procedimientos para el Control de Cambios

1. Prueba e Información del Software

Política: Antes de distribuir cualquier software o información en forma computarizada a terceras personas, los trabajadores de la Empresa X deben

someter el software o la información a una prueba de seguridad, incluyendo una revisión exhaustiva para identificar la presencia de virus en el computador.

Comentario: Esta política evita la responsabilidad por errores o por difundir virus en el software. A pesar de que muchas organizaciones no se consideran editores, esta política puede ser importante si distribuyen software o información en cualquier forma electrónica. Por ejemplo, una empresa de fletes puede suministrar a sus clientes un programa en disco que permita determinar los costos de embarque de carga y número de días para enviar un paquete a un lugar determinado. Esta empresa debe someter el software a las pruebas descritas en esta política. Esta política también se puede ampliar para indicar el cargo de la persona o el departamento encargado de determinar cuáles son las pruebas que pueden aplicarse.

Políticas Relacionadas: “Prueba del Software”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Consumo de Recursos por Programas

Política: Los usuarios de computadores no deben ejecutar o escribir ningún programa de computación o proceso que pueda consumir recursos importantes del sistema o que pueda interferir con las actividades de negocios de la Empresa X.

Comentario: Esta política prohíbe el software que puede perjudicar la capacidad de la Empresa X para procesar adecuadamente sus transacciones de negocios. Los gusanos de computadores quedarían prohibidos por efecto de esta política. Los juegos en Internet pueden consumir una gran cantidad de ancho de banda en la red de trabajo interna, y están prohibidos por esta política. El uso excesivo del sistema es un buen indicador de que existe un virus o algún otro programa o proceso no autorizado. Algunos operadores eliminarán trabajos que consumen recursos en cantidades excesivas, y esta política les proporciona autorización administrativa para hacerlo. Las palabras "proceso" y "programa" se agregaron a esta política para incluir macros, comandos shell y archivos de comandos, que no se consideran programas de computación. Si los usuarios tienen prohibido escribir o ejecutar estos programas o procesos, la administración puede tomar medidas disciplinarias. Además de impedir el experimento con virus, gusanos y software similar, esta política es un freno para aquéllos que gustan de manipular los sistemas de producción de negocios solamente para ver qué pasa.

Políticas Relacionadas: “Consumo Excesivo de Recursos,” “Procesos, Sesiones y Archivos de Usuarios,” y “Envíos de Correos Electrónicos No Solicitados”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

3. Convenciones en Desarrollo de Sistemas

Política: La gerencia debe garantizar que todas las actividades de desarrollo y mantenimiento de software ejecutadas por personal propio suscriban las políticas, las normas, los procedimientos y otras convenciones de desarrollo de sistemas de la Empresa X.

Comentario: Esta política instruye a tanto la gerencia local como la centralizada en el sentido de garantizar que todas las actividades de desarrollo ejecutadas por personal propio cumplen las convenciones normalizadas de desarrollo de sistemas. La creciente popularidad de la programación por parte de los usuarios finales logra que esta política adquiera mayor relevancia porque esos usuarios finales a menudo construyen y alteran los sistemas de aplicación de producción sin hacer pruebas o sin la documentación apropiada. Esto hace que esta política sea particularmente importante para ambientes pequeños como los sistemas cliente-servidor, redes de áreas locales y computadores personales. Aunque la programación por parte del usuario final esté prohibida, o simplemente no se efectúe, existe la necesidad de una política como ésta para garantizar que la gerencia local departamental consistentemente está siguiendo las convenciones de desarrollo de sistemas de la Empresa X. La política asume que dichas convenciones de desarrollo de sistemas han sido previamente especificadas. La palabra "producción" puede ser añadida a la política para limitar su aplicabilidad. Si esto se hace, permitiría el desarrollo no gerenciado de un software no perteneciente a producción, pero una vez que el software se lleve a producción, debería exigirse cumplir las convenciones. También puede ser necesaria una definición de lo que implica "desarrollo de software". Esto puede incluir el desarrollo de nuevas bases de datos, nuevos sistemas expertos y actualizaciones codificadas sincronizadas dentro de múltiples archivos en una red cliente-servidor.

Políticas Relacionadas: “Programas de Aplicación de Usuarios Finales,” “Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas,” y “Seguridad Informática Centralizada”

Política Dirigida a: Todos

Ambientes de Seguridad:Todos

4. Vías de Acceso en Software de Production

Política: Antes de trasladar un software desarrollado internamente al modo de producción, los programadores y demás personal técnico deben eliminar todas las vías de acceso y los privilegios especiales en sistemas.

Comentario: Esta política informa a los programadores y otros que trabajen en el desarrollo de sistemas que deben eliminar todas las vías que podrían ser utilizadas para comprometer la seguridad. A pesar de que algunos programadores pueden querer economizar tiempo en el futuro dejando algunas vías no autorizadas en los sistemas de producción, también están creando una vía que puede ser utilizada por personas no autorizadas para aprovecharse de ella. La política también explícitamente requiere que todas las vías especiales sean debidamente divulgadas en la documentación. Esta política es particularmente importante para aquellos ambientes en donde los usuarios finales elaboran sus propias programaciones, incluyendo computación cliente-servidor, redes de área local, intranet y computadores personales, porque estos nuevos programadores pueden no estar familiarizados con los procedimientos tradicionales de desarrollo de sistemas.

Políticas Relacionadas:“Comprometer Mecanismos de Seguridad para los Clientes” y “Burlado de los Controles de Acceso”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

5. Funcionalidad de los Sistemas

Política: Con la excepción de las reparaciones de emergencia, sólo aquellas funciones descritas en un documento autorizado de diseño de sistemas deben ser incluidas en sistemas de producción computarizada o comunicaciones desarrollados internamente.

Comentario: Las funciones no documentadas pueden representar riesgos graves de seguridad. Por ejemplo, un mecanismo no documentado que permita al programador original evadir los controles de acceso, si fuese retenido en la versión de producción de una aplicación, puede ser utilizado por un usuario no autorizado con malas intenciones. Esta política garantiza que toda la funcionalidad está documentada y aprobada. En este contexto, "sistema" puede ser un sistema completo de computación o comunicación, programas de sistemas o

programas de aplicación. Esta política también puede ser utilizada para disciplinar o despedir a un programador que haya construido una funcionalidad no documentada dentro de un sistema. Esta política se hace más importante a medida que los usuarios van desarrollando sus propios sistemas cliente-servidor, sistemas de redes de área local, sistemas departamentales, intranets y sistemas que vinculen computadores personales.

Políticas Relacionadas:“Vías de Acceso en Software de Production”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

6. Proyectos que Involucran Seguridad Humana

Política: Todos los proyectos internos que involucren riesgos de seguridad humana deben tener la firma de un gerente de proyecto de desarrollo computarizado en los formatos de autorización de la prueba, antes de ser utilizados con propósitos de negocios de producción.

Comentario: Esta política hace que el individuo sea responsable por la inclusión de las medidas de control apropiadas relacionadas con la seguridad. Algunas organizaciones querrán especificar qué significa el término "riesgos de seguridad humana", mientras que otras lo tratan de mantener ambiguo para ampliar su aplicación a circunstancias futuras no previstas. Si una organización escoge ser específica, debe hacer referencia a mociones repetitivas y otros asuntos ergonómicos, no sólo a accidentes severos con heridas personales que se puedan sufrir en un determinado momento.

Políticas Relacionadas:“Controles de Sistemas de Producción,” “Interrupción del Sistema por Seguridad,” y “Contraseñas de Presión”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Medianos y altos

7. Notificación de Problemas en los Sistemas

Política: Los diseñadores y desarrolladores de sistemas son individualmente responsables de notificar a la gerencia del proyecto sobre cualquier problema que pudiese ser causado por las aplicaciones que estén construyendo o modificando.

Comentario: Esta política hace personalmente responsables a los diseñadores y desarrolladores de notificar a la gerencia sobre problemas potenciales asociados con los sistemas que están desarrollando o mejorando. En muchas organizaciones, este personal más técnico no dice nada sobre temas serios como fraude o violación de la privacidad. La gerencia, entonces pondrá un sistema en las operaciones de producción, para después descubrir estos problemas que ya eran conocidos. La tecnología de computación es tan diferente a lo que la gente está acostumbrada, que tienen problemas para imaginarse como operará la nueva tecnología una vez se coloque en producción. Mientras más gente piense sobre los problemas potenciales antes de que un sistema entre en operación de producción, mayor será la probabilidad de que estos problemas sean descubiertos y corregidos antes de que ocurran pérdidas serias.

Políticas Relacionadas: “[Información de Contacto en Seguridad](#)” e “[Informe de Vulnerabilidades del Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Procedimiento de Control de Cambios

Política: Todos los sistemas de computación y comunicaciones utilizados para procesos de producción en la Empresa X deben emplear un procedimiento formal de control de cambios para autorizar todos los cambios significativos al software, hardware, redes de comunicación y procedimientos relacionados.

Comentario: Esta política estabiliza el ambiente en el proceso de producción controlando todos los cambios realizados. Un cambio formal en el control de proceso garantizará que sólo se harán cambios autorizados, que son efectuados en el momento autorizado y que son realizados en la forma autorizada. Esto debe aumentar el porcentaje de tiempo que el sistema está disponible para procesar las transacciones del negocio. Tales cambios en los procesos de control son útiles para requerir la preparación de documentos, lo cual será importante para la solución de problemas y planificación de contingencias. Una definición explícita de "procesos de producción" puede ser un suplemento importante para esta política. Esta política es relevante para sistemas de comunicaciones de voz, tales como correo de voz e intercambios de sucursales privadas y sistemas de comunicación de datos como la intranet. Las licencias de gerencia de software y sistemas de inventarios de hardware se utilizan para suministrar dicho control de cambios para sistemas pequeños como cliente-servidor, redes de área local y computadores personales.

Políticas Relacionadas: “[Cambios en Producción](#)” y “[Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

9. Consideraciones de Seguridad en Cambios en los Sistemas de Producción

Política: Todo cambio a sistemas de producción que no sea de emergencia debe ser consistente con la arquitectura de seguridad informática y estar autorizado por la gerencia como parte del proceso formal de control de cambios.

Comentario: Esta política garantiza que el personal de operaciones de computación y el personal de la administración de sistemas instalarán sólo el hardware y software que son consistentes con un documento de arquitectura de seguridad informática. La política dice que los sistemas de producción sólo pueden ser cambiados de tal manera que cumplan con la arquitectura de seguridad informática. La política establece la importancia de una arquitectura de seguridad informática y especifica algunas de las circunstancias en las cuales debe ser consultada. Debido a que la política se aplica al final del proceso de desarrollo y prueba de los sistemas, implica que los diseñadores y desarrolladores de sistemas ya han considerado la arquitectura. Se requiere un proceso separado si los cambios obedecen a una situación de emergencia. Antes de adoptar una política como ésta, la organización debe escribir y luego obtener autorización de la gerencia para una arquitectura.

Políticas Relacionadas: “[Carga de Programas Externos](#)” y “[Acuerdos de Negocios por Internet](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

10. Controles de Acceso a las Operaciones de Producción

Política: Todos los controles de acceso a nivel de usuario y administrativo requeridos por las políticas de seguridad informática de la Empresa X se deben establecer y habilitar antes de poner en operación los sistemas informáticos de producción.

Comentario: Esta política evita que el personal técnico ponga un sistema en operación de producción, sin tener los controles de acceso definidos dentro de un nivel

razonable. Algunas veces los sistemas son puestos en operación pero los controles de acceso no han sido activados, o si son activados, no están definidos en un nivel seguro. Por ejemplo, en muchos casos, los controles de acceso de contraseñas fijas están definidos, pero se emplean identificadores de usuario grupales. A menos que se utilice un identificador de usuario individual, los registros no mostrarán cuál usuario tomó cuáles acciones y será difícil hacer cumplir la separación de tareas. La política asume que las políticas de control de acceso se han establecido previa o simultáneamente.

Políticas Relacionadas: “Controles de Acceso para Sistemas Remotos” y “Controles de Acceso al Sistema de Computación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

11. Software Innecesario

Política: Las características de software que pudiesen ser utilizadas para comprometer la seguridad y que son claramente innecesarias en el ambiente computarizado de la Empresa X, deben ser inhabilitadas en el momento de ser instalado el software en sistemas multiusuario.

Comentario: Esta política evita que las características innecesarias e inhabilitadas sean utilizadas por los hackers y otros que intentan comprometer la seguridad de los sistemas. Los paquetes de software comúnmente traen muchas características adicionales que las organizaciones no necesitan. Mientras esto es un atractivo para compradores del software, también proporciona vulnerabilidades adicionales que pueden ser aprovechadas por usuarios no autorizados. Esta política puede ser ampliada para aplicar a software en sistemas de un solo usuario, en cuyo caso las palabras “en sistemas multiusuario” deben ser removidas. Nada en la política evita que las características inhabilitadas puedan ser habilitadas posteriormente, si las circunstancias así lo ameritan. A los usuarios se les debe impedir rehabilitar estas características a través de mecanismos de control de acceso y otras medidas de seguridad.

Políticas Relacionadas: “Inhabilitación de Java,” “Vías de Acceso en Software de Producción,” y “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12. Documentación de Cambios en Sistemas de Producción

Política: La documentación que refleje la naturaleza, autorización y desenvolvimiento de todos los cambios significativos a sistemas de producción computarizada y comunicaciones de la Empresa X, debe ser preparada en el lapso de una semana después de efectuado el cambio.

Comentario: El propósito de esta política es requerir que los trabajadores técnicos se adhieran a las fechas de preparación de la documentación. Si no existe una fecha tope para esto, muchas de estas personas se mantendrán posponiendo la preparación de la documentación por períodos de tiempo extensos. Si esto pasa, hay una gran probabilidad que el personal técnico involucrado se haya ido de la organización, hayan sido transferidos a otra posición o simplemente olvidaron el cambio. El no tener la documentación actualizada es también un impedimento para la solución de los problemas diarios, el adiestramiento de nuevo personal, y los esfuerzos de planificación de contingencias y esfuerzos de recuperación de desastres. Si se da al personal técnico una semana para preparar la documentación, la mantiene actualizada y también les permite efectuar cambios de emergencia sin tener que documentarlos. Para algunas organizaciones esta política pudiera parecer ser muy suave. Ellas quizás querrán tener una documentación completa previa al cambio, con la excepción de arreglos de emergencia. Otros querrán que la documentación se prepare antes del cambio. Mientras que algunas organizaciones la encontrarán muy rígida, es también posible evitar que el software se mueva a un ambiente de proceso de producción a menos de que la documentación haya sido preparada.

Políticas Relacionadas: “Documentación de Adiestramiento y Operaciones” y “Cambios del Sistema Operativo de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

13. Documentación de Adiestramiento y Operaciones

Política: Los sistemas de aplicación de negocios en desarrollo o que estén sufriendo modificaciones importantes no deben ser movidos a un ambiente de procesos de producción sin tener materiales adecuados de adiestramiento y documentación de operaciones.

Comentario: Sistemas sin documentación o sistemas operados por personal no adiestrado son muy difíciles de controlar. Al no estar los operadores suficientemente

adiestrados, pueden ocurrir pérdidas importantes. Los desfalcadores y otros empeñados en cometer delitos de computación, frecuentemente se aprovechan de la confusión que hay con un sistema nuevo o sistema que no esté documentado apropiadamente. Con esta política se intenta requerir el adiestramiento adecuado y que la documentación de operaciones se prepare y autorice antes de que el sistema sea formalmente trasladado a producción. Aunque generalmente es más difícil de implantar debido a herramientas menos sofisticadas de seguridad, esta política es aplicable a sistemas pequeños como los cliente-servidor, redes de área local y computadores personales.

Políticas Relacionadas: “Responsabilidades del Usuario de la Información,” “Documentación de Cambios en Sistemas de Producción,” y “Documentación para Sistemas de Producción”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

14. Prueba de Software Externo

Política: Los programas ejecutables que se obtengan de entidades externas deben ser autorizados de acuerdo con las normas de la Empresa X y estar correctamente documentados antes de instalarse en cualquier sistema de producción de la Empresa X.

Comentario: Esta política tiene la intención de evitar que se dañen los sistemas, software y datos de la Empresa X mediante códigos no autorizados. Es común para los hackers modificar programas que se colocan en boletines electrónicos, páginas web de Internet y sitios públicos similares. Esta política se aplica sólo a los sistemas de producción, no a la mayoría de computadores personales y redes de área local. La palabra "producción" debe ser definida previamente. Un proceso de prueba acompañado por un proceso de preparación de documentación tendrá que ser preparado para esta política para que funcione como se pretende. A pesar de que el software de dominio público es el riesgo más significativo aquí, es también una buena práctica el probarlo y examinar los códigos recibidos de proveedores confiables. Esta política está destinada para el personal del departamento de Sistemas Informáticos, en vez de los usuarios finales.

Políticas Relacionadas: “Prueba del Software” y “Exploración del Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

15. Revisión y Recompilación de Software

Política: Los módulos de software probados en su totalidad, deben ser revisados de manera independiente y recompilados antes de trasladarlos a las bibliotecas de producción.

Comentario: Más allá de la detección y corrección temprana de errores y omisiones, esta política evita la incorporación de códigos no autorizados en el software de producción. La política también tiene un elemento de separación de tareas en donde la persona que la revisa no debe ser la misma que realiza las pruebas. La política puede aún ampliarse más para requerir que el probador no sea la misma persona que lo desarrolla. Estos controles de separaciones sólo son posibles en organizaciones grandes que tienen suficiente personal para efectuar diferentes trabajos. Otro propósito de esta política es garantizar que la versión ejecutable de un programa es idéntica al código fuente del programa. Esta política es importante para sistemas cliente-servidor, redes de área local, computadores personales y otros sistemas pequeños a pesar de que es por lo general más difícil de implantar. Otro beneficio de esta política es que requiere la preparación de documentación adecuada para cargarla en el nuevo sistema. Sin esto, otra persona no podrá instalar el nuevo software. El término "recompilación" puede ser modificado para adaptarse a la terminología usada en la organización.

Políticas Relacionadas: “Separación de Tareas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

16. Proceso de Control de Cambios para Aplicaciones de Negocios

Política: Se debe utilizar un proceso formal de control de cambios para garantizar que todo el software de aplicaciones de negocio que sea migrado a producción está autorizado por la gerencia de Sistemas Informáticos y la gerencia de la organización usuaria.

Comentario: Esta política exige un proceso formal y por escrito de control de cambios para el desarrollo de aplicaciones de negocios de producción. Los beneficios de un proceso formal de control de cambios incluyen documentación más reciente, más estabilidad en el sistema y un ambiente estructurado del sistema lo cual lo facilita su control y manejo. Esta política se refiere al requerimiento de un proceso de control de cambios, no a los privilegios utilizados para sostener tal proceso. Una definición de "software de aplicación de negocios"

considerada como de producción puede también acompañar a esta política. El proceso de control de cambios descrito en esta política puede ser extendido a paquetes de software y otras partes de las operaciones de procesamiento de datos. Cualquier palabra adicional explicativa para esta política debe reflejar solamente los componentes esenciales para un proceso formal de control de cambios. Esto es porque existen muchas metodologías y porque los departamentos de Sistemas Informáticos frecuentemente cambian las metodologías. Esta política puede ser utilizada en aquellas circunstancias donde la organización aún no está lista para extender el control de cambios a otras áreas de sistemas informáticos tal como el hardware y comunicaciones. Las palabras "gerencia de la organización del usuario" puede, en algunas organizaciones ser cambiada por las palabras "Propietario de la aplicación".

Políticas Relacionadas:“[Migración de Software](#)” y “[Desarrollo de Sistemas por Usuarios Finales](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

17. Autorización para Cambiar Paquete de Software de Producción

Política: Los cambios al software de aplicaciones suministrados por los vendedores deben efectuarse sólo después de conseguir permiso por escrito de la gerencia de Sistemas Informáticos, siguiendo los procedimientos de control de cambios utilizados para el software de aplicación desarrollado internamente.

Comentario:Esta política requiere que el software empacado por terceros siga el mismo proceso de control utilizado para el software desarrollado internamente. Tales modificaciones pueden comprometer la compatibilidad con las versiones subsiguientes del software, y causar que el vendedor se niegue a dar soporte adicional al software, o causar que el vendedor justificadamente renuncie a tener responsabilidad por el comportamiento del software. Tales cambios pueden causar que el software funcione de manera no autorizada, menos segura o de una manera no deseada. Una versión de esta política puede ser apropiada para usuarios de computadores personales, estaciones de trabajo, redes de área local y sistemas cliente-servidor. La selección de ciertos parámetros durante el proceso de instalación o el proceso que utilice el usuario no constituye un cambio del software.

Políticas Relacionadas:“[Proceso de Control de Cambios para Aplicaciones de Negocios](#)” y “[Servicio Nuevo o Mejorado](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

18. Mantenimiento de Software

Política: Todos los cambios permanentes al software de producción deben ser efectuados utilizando el código fuente.

Comentario:El mantenimiento del código fuente es considerablemente más fácil que el mantenimiento del código objeto. Los cambios en el código objeto conllevan la introducción de nuevos problemas. Es deseable que un recompilador o intérprete verifique la validez del nuevo código antes de su ejecución. Esto no puede ser efectuado si los cambios son hechos directamente en el código objeto. Esta política requiere que los cambios en el software de producción se hagan en la fuente y no en el objeto. Esta política es deseable porque implícitamente requiere que se prepare la documentación para el código fuente.

Políticas Relacionadas:“[Garantía Especial de Software](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

19. Documentación de los Controles de Cambios

Política: La documentación de control de cambios en aplicaciones de producción se debe mantener para que indique qué cambio y cómo, quién hizo los cambios, quién probó los cambios, quién los autorizó, quién los migró a producción y permitió que cualquiera o toda versión anterior de aplicaciones de producción pueda ser fácilmente re-creada.

Comentario:Esta política tiene la intención de resaltar un proceso de control de cambios y la documentación relacionada. No se intenta que se mantenga por sí misma sino que se apoye con documentación de procedimientos de control de cambios. Una significativa separación de tareas esta inmersa en esta política en que personas diferentes están efectuando cambios, probando cambios, migrando cambios y autorizándolos. Esta política asistirá a los auditores e investigadores de delitos de computación en sus esfuerzos por determinar los cambios que las aplicaciones han sufrido a través del

tiempo. La política ayuda en los planes de contingencia porque dice que las versiones anteriores de la aplicación deben estar disponibles, en caso que hubiese la necesidad de regresar a estas versiones anteriores.

Políticas Relacionadas: “Garantía Especial de Software” y “Documentación de Cambios en Sistemas de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

20. Implantación de Cambios en Sistemas Informáticos de Producción

Política: Todos los cambios deben ser comunicados a las personas afectadas por lo menos con dos semanas de anticipación al cambio, y la implantación de todos los cambios que no sean de emergencia deben efectuarse en el primer fin de semana de cada mes.

Comentario: La política no permite cambios frecuentes o sin ser anunciados, ya que ambos pueden causar muchos problemas a los usuarios. Esta política es más importante para aquellas organizaciones que prestan un servicio a otros como transportistas, proveedores de servicios de Internet y proveedores de servicios de aplicaciones. También puede ser utilizada para sistemas grandes multiusuario o redes internas donde hay una variedad de usuarios que desean saber de los cambios que se avecinan. Las organizaciones que adopten esta política deben tener unos planes de contingencia bien desarrollados para manejar los problemas que traen los nuevos cambios. La razón del porqué estos cambios se realizan el primer fin de semana de cada mes, está en que para esa fecha la contabilidad del mes anterior

estará lista y la demanda de servicios será baja. Esta estipulación tendrá que ser modificada dependiendo de los ciclos financieros de la organización.

Políticas Relacionadas: “Proceso de Control de Cambios para Aplicaciones de Negocios” y “Arreglos de Seguridad”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Altos

21. Documentación de Características y Funciones del Software

Política: Todas las características y funciones de software dadas a conocer al público deben estar contenidas en la documentación que se entregue a los usuarios.

Comentario: Esta política evita que los programadores y otros involucrados en los procesos de desarrollo de sistemas incorporen características o funciones que no se han dado a conocer a los usuarios o a la gerencia interna. Para prevenir acusaciones y la pérdida de confianza por parte del cliente, todas las características y funciones deben divulgarse en la documentación. Los usuarios no necesitan cambiar o inhabilitar estas funciones o características; sólo necesitan saber que existen. Esta política es sólo relevante para software distribuido a terceros. Si el software es para uso interno, entonces esta política no será necesaria.

Políticas Relacionadas: “Vías de Acceso en Software de Production” y “Burlado de los Controles de Acceso”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.05.02 Revisión Técnica de los Cambios en Sistemas Operativos

1. Configuración del Sistema Operativo

Política: El personal técnico de la Empresa X debe configurar los servidores de producción con aquellos sistemas operativos que permitan que la función innecesaria o no requerida se elimine completamente.

Comentario: Esta política expresa una preferencia por los sistemas operativos en los cuales los módulos de software que no se necesiten pueden ser removidos y borrados. Esto difiere de los sistemas operativos en los cuales la remoción es muy difícil, o imposible. Se puede decir que lo mejor que los administradores pueden hacer

con algunos sistemas operativos es cerrar algunas funciones o características que no desean. El problema es que los hackers, los espías industriales, empleados disgustados y otros usuarios no autorizados pueden algunas veces habilitarlas nuevamente. Habilitar funciones que no operaban es mucho más fácil que reconfigurar el sistema operativo, y luego reiniciarlo.

Políticas Relacionadas: “Inhabilitación de Componentes Críticos de Seguridad” y “Configuración de Cortafuegos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

2. Parches de Software, Arreglos y Actualizaciones

Política: Todos los sistemas de producción en la red de la Empresa X deben tener un proceso debidamente integrado del personal para, de manera expedita y regular, revisar e instalar todos los nuevos parches, arreglos de errores y actualizaciones de software de sistemas.

Comentario: Esta política garantiza que las redes de una organización y los sistemas no sean penetrados por hackers, espías industriales, terroristas y otros usuarios no bienvenidos. Si el software, especialmente aquel que se utiliza en esos sistemas en la periferia de una red

interna, no es de la última versión, en muchos casos hay errores o problemas de seguridad que los intrusos pueden aprovechar. Si una vulnerabilidad grave se ha anunciado públicamente, entonces el software debe ser inmediatamente actualizado. Esto es especialmente de interés porque ahora está disponible un software de identificación de vulnerabilidades de libre distribución, y los intrusos típicamente usan este software para identificar sistemas que no han sido actualizados recientemente.

Políticas Relacionadas: “[Actualizaciones de Software de Computadores Personales](#),” “[Versiones de Software](#),” y “[Sistemas en Interface con Redes Externas](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

10.05.03 Restricciones en Cambios a Paquetes de Software

1. Instalación de Software de Sistemas Proporcionado por Proveedores

Política: Las nuevas versiones de los sistemas operativos y software de sistemas de producción para computadores multiusuario deben pasar por el proceso de control de cambios establecido antes de ser instalados.

Comentario: El software suministrado por un proveedor no significa que beneficiará a todas las organizaciones usuarias. En algunos casos, las aplicaciones existentes fallarán cuando se instale el nuevo software de sistemas y en otros, la memoria o el límite del espacio en disco causarán problemas cuando el software del sistema se actualice. Esta política evita que el personal de operaciones del computador instale software de sistemas, a menos que el software haya sido aprobado por la gerencia a través del proceso del control de cambios. La política también evita que los programadores de sistemas y otros prueben software nuevo en sistemas de producción, causando una posible corrupción de los datos, una caída de los sistemas y problemas relacionados. Esta política se puede ampliar para incluir aplicaciones suplidadas por proveedores externos y para incluir sistemas de producción de uso individual, pero en la mayoría de los casos, los sistemas de uso individual no tienen sistemas efectivos de control de cambios.

Políticas Relacionadas: “[Proceso de Control de Cambios para Aplicaciones de Negocios](#)” y “[Cambios en Producción](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Acceso de Proveedor Tercero a Software Empacado

Política: Los paquetes de software de terceros que la Empresa X utilice en los sistemas informáticos de producción, deben estar libres de mecanismos de desactivación que pudiesen ser disparados por el proveedor sin el consentimiento de la Empresa X.

Comentario: Esta política evita que la Empresa X se encuentre en posición de dependencia de un tercero para el uso de software crítico, porque éstos pueden desactivar el software y obligar a la empresa a tomar algún tipo de acción. Este tipo de funcionalidad ha sido incorporado a algunos paquetes de software, pero se ha comprobado que es perjudicial para la organización usuaria. Como resultado, su uso se discute en publicaciones de sistemas informáticos. El mecanismo puede ser implantado mediante una variedad de técnicas incluyendo un cronómetro computarizado, un contador de ejecución o un interruptor de acceso remoto para prender o apagar. La política puede ser reforzada añadiéndole estas palabras, “Todo contrato con proveedores externos de software, debe incluir una garantía de que no existe una desactivación funcional controlada por el proveedor”. Aunque organizaciones más pequeñas tendrán problemas para incluir palabras como éstas en un contrato, clientes mayores tendrán el poder para cambiar los contratos normales de licencia

de los proveedores. Esta política no es aplicable a la contratación externa de servicios de información, como las suplidadas por un proveedor de servicio de aplicaciones.

10.05.04 Canales Secretos y Código Troyano

1. Uso de Herramientas y Lenguajes de Software

Política: Los diseñadores y desarrolladores de sistemas de la Empresa X no deben utilizar herramientas y lenguajes de software que no posean atributos comprobados de seguridad cuando construyan páginas web, extranets o cualquier otro sistema que tenga interface con terceros, a menos que se obtenga una aprobación previa de la gerencia de Seguridad Informática.

Comentario: Esta política estimula a los diseñadores y desarrolladores a considerar cuáles herramientas y lenguajes de software se han comprobados como seguros. La delineación entre comprobado y no comprobado como seguro, no es cuantitativa o lógicamente irrefutable sino el resultado de consultas con la gerencia de Seguridad de Informática. La política está restringida a una interface externa, donde los hackers o espías industriales pueden entrar, y no se aplica a los sistemas internos.

Políticas Relacionadas: “Herramientas y Técnicas de Desarrollo Maduras” e “Interfaces a Redes Externas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Enunciados de la Integridad del Software

Política: Si se está considerando la compra de un software a terceros, la gerencia debe obtener una declaración escrita de integridad por parte del proveedor

Políticas Relacionadas: “Software Innecesario” y “Procedimientos de Retorno”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

involucrado, la cual debe garantizar que el software no contiene características que no se han documentado, que no contiene mecanismos ocultos que puedan ser utilizados para comprometer la seguridad del software, y que no requerirá ni el cambio ni el abandono de los controles presentes en el sistema operativo afectado.

Comentario: Esta política obtiene una garantía por escrito de los proveedores externos de software indicando que el software se desempeña de acuerdo a lo ofrecido, y que el mismo no incluye otros mecanismos que puedan servir para evitar la seguridad. Esta garantía por escrito podrá ser utilizada posteriormente en un juicio si se demuestra que el software del proveedor contiene códigos maliciosos. El proceso de requerir y obtener una declaración de integridad, le indica al proveedor que la organización compradora es seria en lo que respecta a seguridad, y que tiene la intención de que el proveedor cargue con la responsabilidad de la integridad de su producto. Algunas organizaciones desearían ampliar esta política para incluir un requerimiento en el sentido de que el proveedor arregle cualquier problema mayor de seguridad que la organización compradora descubra, quizás dentro de cierto período de tiempo. A pesar de que esta política está redactada para sistemas de aplicaciones, la misma puede aplicarse a software de sistemas.

Políticas Relacionadas: “Comprometer Mecanismos de Seguridad para los Clientes”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

10.05.05 Desarrollo de Software con Terceros

1. Desarrollo de Software por Terceros

Política: Los terceros que desarrollen software para la Empresa X quedan obligados por un contrato que incluye, sin limitantes, definiciones claras y precisas de

arreglos de licencia, expectativas de precisión y calidad, acuerdos de garantías, procedimientos de auditoría y requerimientos de pruebas.

Comentario: Esta política garantiza que todo el software desarrollado por terceros para la Empresa X, se completará de acuerdo con los términos y condiciones

estipulados en el contrato. Esto obligará a los terceros a mantener los niveles de expectativa de la Empresa X con respecto a la funcionalidad y calidad del software. También obliga a los terceros a suministrar un producto libre de códigos maliciosos. Si algún aspecto del software no cumple con las normas o expectativas de la Empresa X, la obligatoriedad de un convenio firmado suministra a la Empresa el soporte legal necesario para resolver cualquier disputa.

Políticas Relacionadas: “[Aprobación de Contratos Externos](#),” “[Transferencia de Información a Terceros](#),” “[Sistemas de Producción y Herramientas de Software](#),” y “[Enunciados de la Integridad del Software](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11 GESTIÓN DE CONTINUIDAD DE NEGOCIO

11.01 Aspectos de Gestión de Continuidad de Negocio

11.01.01 Proceso de la Gestión de Continuidad de Negocio

1. Requerimientos para el Soporte de Emergencias y Desastres

Política: Todas las subsidiarias, divisiones, departamentos y otras unidades organizativas que requieran soporte del departamento de Sistemas Informáticos con prioridad en caso de una emergencia o desastre, deben implementar hardware, software, políticas y procedimientos relacionados que sean consistentes con las normas de la Empresa X.

Comentario: Los sistemas fuera de norma dificultan mucho la preparación y el mantenimiento de una política de contingencia, porque el material preparado de planificación de contingencia no se puede utilizar, y porque es menos probable que esté disponible la experiencia interna. Esta política notifica a las unidades de la organización que la gerencia de sistemas de informática no podrá apoyarlos con el mismo alcance de lo que sería posible con unidades organizacionales que sí cumplen las normas internas. Algunos consideran que la política es una herramienta excepcionalmente efectiva para obligar a las unidades de la organización a cumplir las normas de tecnología informática. La política es efectiva en los esfuerzos por centralizar de nuevo la seguridad informática que se ha dispersado entre muchas organizaciones y, en algunos casos, con resultados poco efectivos.

Políticas Relacionadas: “[Dispersión de Sistemas Computacionales](#)” y “[Seguridad Informática Centralizada](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Accesibilidad del Plan de Contingencia

Política: Los planes de contingencia de los sistemas informáticos deben estar accesibles de manera continua en Internet, por lo menos en dos sitios diferentes, apoyados por proveedores diferentes de servicios en Internet.

Comentario: Esta política garantiza que la versión más reciente de los planes de recuperación seguirá estando disponible, a pesar de lo que pudiera ocurrir en las oficinas, computadores, redes, y otras instalaciones de la Empresa X. Si, por ejemplo, el edificio sede de la Empresa X fuese destruido, la política de contingencia más reciente estaría disponible de inmediato para cualquier persona autorizada que tuviere un computador con conexión a Internet. El software de replicación de datos también se puede usar para asegurar que los computadores del personal autorizados tengan la última versión de los planes almacenados en su disco duro. Esto se puede lograr cada vez que uno de estos computadores remotos se conecte. Si los planes de contingencia han sido actualizados, entonces la última versión de los planes serán automáticamente descargados a través del software de replicación de datos. Un formato de archivo normalizado se puede utilizar para almacenar los planes de tal manera de poder ser visualizados en casi cualquier computador.

Políticas Relacionadas: “[Equipo de Respuesta Ante Emergencias Computacionales](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11.01.02 Análisis de Contingencias del Negocio y su Impacto

1. Clasificación de la Criticidad de las Aplicaciones Multiusuario

Política: Conjuntamente con los Propietarios de la Información, la gerencia del Sistemas Informáticos debe preparar o revisar periódicamente una evaluación del nivel de criticidad de todas las aplicaciones de producción en computadores multiusuario.

Comentario: El proceso mediante el cual los niveles de criticidad son asignados a las aplicaciones, constituye un paso previo necesario para diseñar un plan de contingencia efectivo. Esta política requiere, a la luz de esa dependencia, que la gerencia de Sistemas Informáticos o la gerencia de Seguridad Informática, prepare o revise una lista de aplicaciones críticas. A medida que cambien

los sistemas del negocio, también cambiará la criticidad de los sistemas. Asimismo, algunas aplicaciones serán retiradas, otras introducidas, algunas adquieren más importancia y otras, menos. Como resultado de estos y otros cambios, los planes de contingencia deberían ser periódicamente actualizados. Esta política reconoce que la gerencia del departamento usuario indicará que sus sistemas son críticos cuando en realidad no lo son. Para tener una perspectiva consistente y razonable a lo largo de una organización, con frecuencia es necesaria una autoridad central para realizar la evaluación. Esta política aclara que tanto gerencia de Sistemas Informáticos como los Propietarios de los mismos, son responsables de la producción de un informe que muestre la criticidad de las aplicaciones. Esta política supone que el término "producción" ha sido definido con suficiente claridad en otros documentos. La política también supone la existencia de otra política que define el término "crítico".

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” “Planes de Seguridad Informática,” y “Clasificación de Recursos Informáticos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones

Política: Todas las aplicaciones de producción en computadores deben ser ubicadas en una de las cinco clasificaciones de criticidad, cada una con requisitos de manejo diferente: altamente crítico, crítico, prioridad, requerido y diferible.

Comentario: Esta política especifica las categorías de criticidad normalizadas a ser utilizadas en toda la organización. Una vez que se logre la normalización, se puede asignar una categoría a cada aplicación, y las más críticas pueden recibir atención especial durante la planificación de contingencias. La cantidad de categorías de criticidad pueden variar de una organización a otra, así como el significado de los términos como "prioridad." Generalmente, para cada una de ellas se fija un plazo para recuperar la aplicación. Por ejemplo, las aplicaciones "altamente críticas" pudieran ser aquellas que deberían recuperarse en 15 minutos. La

información se puede calificar según el concepto de criticidad, pero debido a que la información con frecuencia es procesada en muchas aplicaciones, es preferible concentrar la atención en una aplicación a la vez, cuando se prepara el plan de contingencia.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Clasificación de la Criticidad de las Aplicaciones Multiusuario,” e “Información y Software Esenciales”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Análisis del Impacto sobre el Negocio

Política: Concluida la evaluación de riesgo a lo largo de la organización, la gerencia de Seguridad Informática, o a quien se delegue, debe hacer un análisis del impacto sobre el negocio que precise la duración del tiempo máximo que la Empresa X puede tolerar la ausencia de los servicios informáticos críticos, el plazo en el cual la gerencia ha de decidir el sitio alternativo de procesamiento, y sobre la configuración de los sistemas mínimos aceptables para la recuperación de los sistemas informáticos de producción.

Comentario: El propósito de esta política es requerir la ejecución, no sólo de una evaluación de riesgo anual o evaluación de riesgo, sino también requerir un análisis anual del impacto sobre el negocio (BIA, Business Impact Analysis). Un BIA es de mucha importancia para efectos de la planificación de contingencias, ya que especifica las diferentes consecuencias de varios tipos de tiempo de caída del sistema o la no disponibilidad del mismo. Un BIA también sirve para medir las consecuencias a través del tiempo. Sólo cuando la gerencia disponga de esta información, podrá tomar decisiones lógicas y con fundamento acerca del traslado a un sitio alternativo. El designado para gerenciar la Seguridad Informática pudiera ser una organización contratada o unos consultores en planificación de contingencias.

Políticas Relacionadas: “Evaluación de Nuevas Tecnologías” y “Evaluación del Riesgo en los Sistemas de Producción”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

11.01.03 Redacción e Implantación de Planes de Contingencia

1. Clasificación de Recursos Informáticos

Política: La Gerencia de Operaciones de Computación conjuntamente con los Propietarios de la Información, deben establecer y utilizar un marco de referencia para clasificar todos los recursos de información, mediante el establecimiento de prioridades de recuperación que permitan que los recursos más críticos sean los primeros en ser recuperados.

Comentario: Esta política especifica cuál unidad de la organización es responsable por definir las categorías y el marco de referencia en general para establecer las prioridades de los recursos informáticos. Esto permitirá la más ágil coordinación de los varios planes de contingencia, fusionarlos, y asignarles prioridades. Las palabras "Operaciones de Computación" pudieran fácilmente ser cambiadas por "Seguridad Informática" u otro grupo organizativo. El marco de referencia pudiera incluir las categorías semejantes a "misión crucial se debe recuperar dentro de una hora", "crucial se debe recuperar dentro de ocho horas" y "todas las otras se deben recuperar en 48 horas".

Políticas Relacionadas: ["Clasificación de la Criticidad de las Aplicaciones Multiusuario"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Preparación y Mantenimiento de Planes de Contingencia Empresarial

Política: La Gerencia debe preparar y periódicamente actualizar y con regularidad poner a prueba, una política de recuperación de negocios que especifique el uso de instalaciones alternativas para que los empleados puedan continuar las operaciones en caso de interrupción del negocio.

Comentario: Un plan de contingencia de negocios tiene que ver con asuntos relativos a las instalaciones y otros aspectos del negocio, aparte de los sistemas de computación y de comunicaciones. Un plan de contingencia para computación y comunicaciones es mucho más estrecho en su alcance. Esta política tiene la intención de suplementar la política relativa a los planes de recuperación ante desastres, porque se necesitarán las instalaciones si la organización ha de mantenerse operativa. Los trabajadores a cargo de crear los planes de contingencia a menudo son distintos de los responsables de los planes de contingencia en sistemas. Por ejemplo, los especialistas de seguridad física pueden idear los planes de contingencia del negocio mientras que los técnicos informáticos crearían los planes de contingencia de los sistemas. Sin embargo, se recomienda una política que exija la creación de planes de contingencia para el negocio, especialmente donde existan mayormente subsidiarias y otras estructuras gerenciales descentralizadas.

Políticas Relacionadas: ["Planes de Recuperación Ante Desastre Computacional"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11.01.04 Marco para la Planificación de la Continuidad del Negocio

1. Plan de Continuidad de Negocios y Computación

Política: La gerencia de Sistemas Informáticos debe documentar y mantener un proceso normalizado para toda la organización para el desarrollo y mantenimiento tanto de las políticas de contingencia del negocio como los planes de contingencia para computación.

Comentario: Esta política requiere la existencia de un proceso formal para la preparación de tanto planes de contingencia del negocio como de computación que

deben ser documentados y mantenidos por la gerencia de Sistemas de Computación. Para poder cubrir una variedad de sistemas más amplia, el plan pudiera cambiar para orientarlos a "planes de contingencia de comunicaciones y de computación" en lugar de limitarse a "planes de contingencia de computación." El proceso de planificación en sí, normalmente hubiera involucrado tales áreas como: identificación y categorización de los procesos cruciales del negocio, identificación de los riesgos que enfrenta la organización, valoración del impacto en potencia de los varios tipos de emergencias

y desastres, identificación y designación de responsabilidades para el manejo de emergencias y desastres, documentación de los procedimientos y proceso, educación del equipo, y sometimiento a prueba de los planes. El plan pudiera expandirse para incluir la mención de tales actividades específicas. Un grupo de Seguridad de Información pudiera definir el proceso normativo mencionado en el plan, aunque Tecnología, Gerencia de Riesgos, Seguros, Planificación de Operaciones, u otros departamentos podrían encargarse de lo mismo.

Políticas Relacionadas: “[Clasificación de Recursos Informáticos](#)” y “[Excepciones a las Políticas](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio

Política: Se espera la presencia de los empleados y su mejor ayuda en la restauración de la actividad normal de las operaciones del negocio de la Empresa X, después de que éstas hayan sido interrumpidas por una emergencia o desastre.

Comentario: Se requiere la presencia de los empleados para ayudar con sus mejores esfuerzos, en la restauración de la normalidad de las operaciones del negocio, inclusive el restablecimiento de los servicios de computación y comunicaciones. Algunas organizaciones incluyen un plan semejante en el manual del empleado para asegurar que no quede duda sobre lo que se espera de ellos en tiempos estresantes. En caso de un desastre, algunos empleados quisieran ofrecer sus servicios voluntarios de socorro. Esta política les informa que deben atender los asuntos de la Empresa X. Otros empleados pudieran protestar que no es de su incumbencia el asistir a la recuperación del negocio. Este plan disipa las disputas sobre el particular. No sería razonable esperar que los empleados consideraren su trabajo más importante que los bienes personales o su familia, de modo que pudiera ampliarse la política en reconocimiento de la necesidad de comprobar la seguridad de los bienes del personal y de sus familias. Este plan se dirige únicamente a la situación de los empleados. Los contratistas, temporales y consultores no tienen obligación de asistir de la misma manera, ya que no tienen el mismo vínculo con la Empresa X.

Políticas Relacionadas: “[Equipo de Respuesta Ante Emergencias Computacionales](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11.01.05 Pruebas, Mantenimiento y Re-Evaluación de los Planes de Continuidad del Negocio

1. Reversión a Procedimientos Manuales

Política: Si las actividades cruciales del negocio de la Empresa X pudieran ser razonablemente realizadas con procedimientos manuales, en lugar de computadores, un plan de contingencia de computación manual tendrá que ser desarrollado, probado, periódicamente actualizado, e integrado con los planes de contingencia del sistema de computación y de comunicaciones.

Comentario: Esta política instruye a la gerencia a considerar el apoyo de las actividades cruciales del negocio con el uso de procedimientos manuales. Algunas personas pierden la perspectiva y, en este caso, piensan que las actividades del negocio sólo se apoyan en la computación. Este plan obliga a la gerencia a probar el desarrollo manual de las actividades normales del negocio. Por ejemplo, el punto de alquiler de automóviles en un aeropuerto encontraría dificultades en el trabajo sin apoyo de computación, pero con toda probabilidad, podría continuar sus operaciones de

manera manual. En este caso, los empleados podrían tener acceso a procedimientos manuales a seguir, si se cayera el sistema. Estos procedimientos también pudieran requerir listas de precios y otra información de salida impresa con la suficiente frecuencia para poder referenciar copias duras cuando se caiga el sistema. Algunas organizaciones pudieran preferir la expansión para requerir ciertos tópicos en procedimientos manuales en el plan de procedimientos manuales de contingencia. Estos procedimientos manuales pudieran ser los pasos iniciales en un plan de recuperación del negocio. Cuando éste sea el caso, una política de contingencia pudiera abarcar la información específica que los usuarios han de documentar manualmente, cuáles actividades pudieran ser realizadas, y cuáles serían las restricciones correspondientes.

Políticas Relacionadas: “[Planes de Recuperación Ante Desastre Computacional](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos**2. Rotación del Personal Fuera de Sede**

Política: Los empleados que participen en operaciones de recuperación fuera de sede con sistemas informáticos de la Empresa X, deben ser rotados regularmente para permitir que por lo menos dos personas tengan los conocimientos técnicos necesarios para realizar cada una de las tareas esenciales de recuperación.

Comentario:Este plan informa a quienes están dirigiendo las actividades de recuperación fuera de sede, que deben incorporar el proceso de rotación de tareas en sus labores. Algunas veces la rotación de tareas no se toma en cuenta, lo que deja a una organización crucialmente dependiente de unas cuantas personas técnicas, y si estas pocas personas no estuvieran de pronto disponibles, entonces las operaciones de recuperación serían difíciles de realizar, requiriendo mucho tiempo y recursos financieros. Existen investigaciones que revelan que el 40% de las empresas pequeñas no pueden abrir sus puertas al público después de un desastre como un tornado, un terremoto o una inundación. Esto ocurre principalmente porque falta suficiente documentación y adiestramiento multidisciplinario. Si este adiestramiento y la rotación de tareas fuesen obligatorios, el hecho también incentivaría poderosamente el desarrollo actual de la documentación de recuperación. Esta política exige que los involucrados en la planificación de la recuperación impartan carácter esencial a ciertas tareas.

Políticas Relacionadas:“[Puestos Técnicos Esenciales](#)” y “[Rotación de Trabajo](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos**3. Niveles de Soporte de Interrupción del Negocio**

Política: Anualmente, las gerencias de los departamentos usuarios y de Tecnología Informática han de convenir y documentar los niveles de apoyo que serán suministrados en caso de desastre o emergencia.

Comentario:Esta política establece el tipo de apoyo técnico y administrativo que será prestado en caso de un desastre o emergencia. Por ejemplo, los departamentos que usan aplicaciones que no son altamente cruciales, no serían restaurados simultáneamente con otros departamentos. Esta política protege a la gerencia de Tecnología Informática o a quien esté preparando un plan de contingencia porque documenta los niveles

apropiados de apoyo. Si estos requisitos están plasmados en papel, los usuarios no podrán responsabilizar a Tecnología Informática por ciertos problemas acerca de los cuales hayan sido advertidos, y estarán motivados a prestar más atención a la planificación de contingencias. En las primeras etapas del desarrollo de la política de contingencia, un plan como éste pudiera abrigar la realización de una evaluación de riesgo para determinar el impacto del desastre o emergencia. Este plan pudiera ampliarse para requerir que estos niveles de apoyo sean revisados anualmente. Esto sería recomendable si se tuvieran que hacer muchos cambios en los sistemas informáticos. Precisamente por la autonomía en el proceso de toma de decisiones, este plan es particularmente importante para aquellas organizaciones que dependen de sistemas cliente-servidor, redes de área local y otros sistemas distribuidos de computación.

Políticas Relacionadas:“[Requerimientos para el Soporte de Emergencias y Desastres](#),” “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#),” y “[Mantenimiento Preventivo](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos**4. Prueba del Plan de Contingencia**

Política: Los planes de contingencia para los sistemas de computación y comunicación deben ser probados rutinariamente, y seguidos de un breve informe para la alta gerencia con los detalles de los resultados.

Comentario:Esta política requiere una prueba periódica de los planes de contingencia. La confianza en poderse recuperar después de un desastre o de una emergencia se logra mediante la regularidad de pruebas. El personal de planificación de computación y contingencias pudiera ser cambiado, de manera que las pruebas periódicas son necesarias con el fin de garantizar que las estrategias y procedimientos previamente desarrollados para la recuperación serán pertinentes. El requerimiento de un informe para la alta gerencia la mantiene informada acerca de los planes de contingencia, requiere que el trabajo sea documentado e incentiva las pruebas y ajustes a los planes de contingencia. Si aún la organización no goza de un plan de contingencia, entonces la política no es aplicable. Algunas organizaciones pudieran desear que la política fuese más estricta, en cuyo caso se puede establecer un plazo para la prueba. Es recomendable que se hagan las pruebas a intervalos regulares, en lugar de hacerlas al azar, aunque sea menos realista. Es importante que requiera de quienes

hagan las pruebas informen sobre las deficiencias, aunque éstos no tengan los recursos o el permiso de gerencia para realizar las reparaciones o ajustes necesarios.

Políticas Relacionadas:“[Planes de Recuperación Ante Desastre Computacional](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

5. Prueba de Números Telefónicos

Política: Cada trimestre, el equipo de Seguridad Informática deberá probar y revisar un árbol de llamadas, en el cual se indiquen todos los números de teléfonos disponibles para cada uno de los empleados involucrados en la planificación de contingencias relacionadas con los sistemas informáticos, y respuesta ante desastres y emergencias.

Comentario:La política requiere la prueba periódica y la actualización de un árbol de llamadas, el cual muestra los números de teléfono, inclusive el correo de voz, de habitación y los nombres, y a veces, las áreas de responsabilidad. Debido a que los empleados cambian de trabajo, residencia y número de teléfono, es importante asegurar que un árbol de llamadas contenga información actualizada. Cuando ocurre un desastre o emergencia, no es el momento para estar llamando a la central de información para convencer a la operadora de que un número reservado de hecho, debería ser divulgado. Un árbol de llamadas con frecuencia será parte de la documentación del equipo de respuesta ante emergencias computacionales (CERT), pero será necesario aún en ausencia de un CERT. El árbol de llamadas incluye a los que hacen la planificación, no sólo a los que tengan la responsabilidad de manejar la respuesta; lo que significa que todo el personal involucrado pueda ser contactado cuando sea necesario.

Políticas Relacionadas:“[Información de Contacto](#)” y “[Números de Acceso a Computadores](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

6. Roles en la Planificación de Contingencias y Recuperación de Sistemas

Política: Las funciones y responsabilidades para tanto los sistemas de planificación de contingencias como de recuperación de sistemas, deben ser revisadas y actualizadas anualmente por la gerencia de Seguridad Informática.

Comentario:Esta política asigna las responsabilidades en la revisión y actualización de las funciones y responsabilidades de planificación de los sistemas de contingencias. A veces, estas funciones y responsabilidades configuran una descripción de tareas y para la documentación de procedimientos para equipos de respuestas ante emergencias computacionales, pero también pueden figurar en una gran variedad de otros documentos. En algunas organizaciones, la responsabilidad de la revisión y actualización de estas funciones y responsabilidades no están claramente asignadas, y debido a que la planificación de contingencias y la recuperación de sistemas, por su propia naturaleza, son multi-departamental y multi-funcional, esta tarea pudiera ser completada con dificultad.

Políticas Relacionadas:“[Comité de Gestión de Seguridad Informática](#)” y “[Administradores de Seguridad Suplentes](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

12 CUMPLIMIENTO

12.01 Cumplimiento de Requisitos Legales

12.01.01 Identificación de la Legislación Pertinente

1. Reglamentos y Requisitos

Política: Todos los requisitos estatutarios, regulatorios y contractuales, tienen que ser definidos y documentados para cada sistema informático de la Empresa X.

Comentario: Esta política garantiza que todos los sistemas informáticos cumplirán los requisitos estatutarios, regulatorios y contractuales pertinentes. Los reglamentos son adoptados constantemente para requerir controles de seguridad sobre aplicaciones específicas de información. Algunos incluyen las prohibiciones de divulgación de información de cuentas

de clientes, normas para proteger la seguridad y confidencialidad y la notificación anual al cliente sobre la privacidad. Esta política exigirá que el desarrollo de estos sistemas informáticos tome en cuenta la totalidad de todos los requisitos, los implementen y los documenten.

Políticas Relacionadas: “[Avisos de Derechos de Autor en Software](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

12.01.02 Derechos de Propiedad Intelectual

1. Fuente de Desarrollo de Software

Política: El software que soporte las aplicaciones de negocios de producción debe ser desarrollado internamente o adquirido de algún proveedor tercero reconocido y confiable.

Comentario: Esta política evita que los empleados descarguen software gratuito de Internet, ya que algunos pueden contener códigos maliciosos. La política también evita que el ambiente de computación se construya con tecnología que pudiera no ser actualizada regularmente, que pudiera no ser robusta, y que no estuviese apoyada por una empresa solvente. El software gratuito también puede introducir lo incompatible con resultados inesperados en lo que de otra manera es un ambiente de computación estable. Este es otro motivo para ser firme en la prohibición contra el software gratuito. Si bien existen paquetes gratuitos disponibles en el Internet, cada uno de estos paquetes deben ser bien evaluados antes de permitirse su uso en las máquinas de producción. La evaluación típicamente debería determinar que una buena documentación esté disponible, que adiestramiento apropiado esté disponible, que haya apoyo técnico disponible a solicitud, que las actualizaciones sean regularmente suministradas, y que el proveedor muestre un negocio financieramente estable. Esta línea se puede implementar con software de control de cambios en el computador personal que pueda evitar que los usuarios

finales efectúen algún cambio en el software operativo de su computador, excepto cuando sea autorizado por los administradores aprobados.

Políticas Relacionadas: “[Prueba de Software Externo](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

2. Sistemas de Producción y Herramientas de Software

Política: Los sistemas informáticos de producción de la Empresa X, sólo debe hacer uso de aquellas herramientas que hayan sido legítimamente desarrolladas por proveedores fiables, asociaciones profesionales, agrupaciones gremiales o agencias gubernamentales.

Comentario: Esta política garantiza que la Empresa X hará uso sólo de software legítimo de proveedores que hayan demostrado ser seguros y confiables. Si la organización no da importancia al software que carga y usa para los sistemas de producción, podría introducir códigos maliciosos que dañen el sistema. Esta línea evita que la organización sea engañada por terceros mediante la oferta de software, particularmente un software compartido o gratuito, pretendiendo así introducirse a los sistemas de la organización. Esta

política tiene la finalidad de evitar que los administradores del sistema, y otros, sencillamente descarguen de Internet lo que creen es software útil, sólo para descubrir después que contiene un código malicioso incrustado en el mismo. Esta política no contempla la situación en la cual paquetes de software suministrados por un proveedor aprobado pudiera contener un código incrustado por terceras personas no autorizadas.

Políticas Relacionadas: “Prueba de Software Externo” y “Fuente de Desarrollo de Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Garantía Especial de Software

Política: Si se ha de usar software de terceros para una actividad crítica de negocios, el proveedor debe otorgar licencia de código de fuente a la Empresa X o debe conceder acceso al código fuente por medio de un convenio de plica (o de custodia en garantía) con dicho tercero.

Comentario: En ciertas condiciones definidas contractualmente, el convenio de plica permite a la organización compradora el acceso a un código previamente restringido, en caso de que el proveedor no satisfaga las condiciones contractuales o que liquide su negocio. Esta política es aplicable a una gran variedad de relaciones comerciales con un tercer proveedor de software, inclusive el arrendamiento, alquiler y compra. Esta política también puede ser apropiada en aquellos casos cuando se emplea un proveedor de servicios de aplicación o algún tipo de organización contratada. En esta política, las palabras "actividad crítica de negocios" son deliberadamente ambiguas para que puedan ser aplicadas a una amplia gama de software. Para aquellas organizaciones de gran escala, el alcance de la política pudiera ser ampliada para incluir sistemas de software, pero el método es poco utilizado. Para efectos de una definición de la palabra "crítica", esta política asume la existencia de una política aprobada de clasificación de datos.

Políticas Relacionadas: “Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones,” “Software Distribuido a Terceros,” y “Mantenimiento de Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

4. Verificación de Software En Garantía Especial

Política: Para cada puesta en circulación importante de software crítico para los negocios de la Empresa X y que un tercero la tenga en plica, un tercero independiente debe verificar que el agente de plica (o custodio garante) haya recibido todo el software necesario y su documentación.

Comentario: Esta política asegura que los arreglos de plica del software existentes brindan la protección necesaria. Si todos los materiales necesarios no están depositados en los predios del agente de plica, la Empresa X pudiera tener dificultades si el proveedor del software liquida su negocio, descontinúa algún producto, se niega a reparar algún error o de otra manera está en violación de un convenio celebrado con la Empresa X. La existencia de esta política idealmente se comunica tanto al proveedor del software como al agente de plica antes de establecer tal acuerdo de software. La política instará a ambos a ceñirse al estricto cumplimiento de los términos y condiciones del contrato. En lugar de esta política, algunas organizaciones pudieran sentir más seguridad con informes del agente de plica en los cuales se plasme lo que hayan recibido. Otras organizaciones, al igual a las que adopten una política como ésta, querrán hacerse de servicios de terceros independientes para verificar los materiales que hayan sido depositados en las instalaciones del agente de plica. Este agente no puede permitir el acceso a los materiales en plica, a los empleados de la organización usuaria. Esta norma puede requerir el uso de auditorías externas.

Políticas Relacionadas: “Garantía Especial de Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

5. Atribución de la Información

Política: Los trabajadores de la Empresa X siempre deben acreditar de manera apropiada a la fuente de información utilizada para propósitos de la Empresa X.

Comentario: Esta política apoya a la gerencia en la evaluación y confiabilidad de la información que se presenta para su aprobación. La política, adicionalmente, alerta a la gerencia de la existencia de derechos a la información que pudieran haber sido ignorados por algún trabajador en la preparación de un informe o en el desarrollo de un producto nuevo. Este comportamiento reduce la incidencia de alegatos de que la Empresa X se

apropió indebidamente de cierta información. Esta política también promueve una actitud respetuosa de los derechos de la propiedad intelectual, que puede ser de importancia cuando hay que disuadir el copiado de software sin autorización y otros abusos respecto de la propiedad intelectual. Adicionalmente, esta política promueve el uso responsable de Internet y de otros foros electrónicos; porque los empleados serán menos propensos a colocar información después de eliminar referencias a una fuente.

Políticas Relacionadas: “Etiquetado de la Propiedad Intelectual” e “Identidades Falsas”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

6. Etiquetado de la Propiedad Intelectual

Política: Todos los usuarios que presenten información para la cual no poseen el derecho de autor o de cualquier otro derecho en el área pública del sitio web de la Empresa X, o en el sistema de foros electrónicos, deben identificar claramente la fuente de la información.

Comentario: Esta política aclara la atribución de derechos sobre la información y evita una situación ambigua. Esta también aclara la designación de responsabilidades para especificar los derechos de propiedad de la información presentada en un área de dominio público. La política transfiere el derecho al operador del sitio o del sistema de foros electrónicos (BBS, por sus siglas en inglés) para usar la información desplegada para fines de mercadeo y otras razones sin necesidad adicional de autorización o pago de regalías. Esta política, en lugar de ser pertinente sólo a los sitios y al BBS, también es apropiada para cualquier sistema multiorganizacional, tales como los servicios en línea.

Políticas Relacionadas: “Atribución de la Información” y “Etiquetado de Datos Usados Como Base de Decisión Gerencial”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7. Avisos de Derechos de Autor en Software

Política: Todos los programas de computación y documentación de programación que sean propiedad de la Empresa X deben ser incluidos en los avisos de derechos de autor correspondientes.

Comentario: Aunque en ciertas jurisdicciones no es necesario hacer mención explícita de los derechos de autor para que sean de cumplimiento forzoso, la existencia del aviso surte un efecto disuasivo. Por otra parte, otras jurisdicciones sí pueden requerir avisos explícitos. También se puede hacer mención de la política en los lugares donde han de aparecer los derechos de autor. Por ejemplo, los avisos pudieran aparecer como visualizaciones en pantalla, listas de fuentes de códigos, listas de códigos de objetos o en manuales del usuario. La política también puede ser ampliada para incluir la redacción necesaria en una jurisdicción en particular. En algunos casos, las palabras "La Empresa X Se Reserva El Derecho Sobre Estos Archivos Electrónicos" pueden ser también necesarias para restringir la inserción no autorizada del material en bases de datos en línea.

Políticas Relacionadas: “Derechos de Propiedad Intelectual”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

8. Copias Múltiples de la Información

Política: Los trabajadores no pueden hacer copias múltiples del material extraído de alguna publicación, excepto cuando se haya obtenido el permiso del Propietario de los derechos de autor o sólo cuando esto sea razonable y acostumbrado.

Comentario: Esta política ataja los problemas de derechos de autor antes de que se conviertan en queja formal. La intención es la de comunicar el significado del término legal "uso justo," que permite hacer copias sin compensación al Propietario del derecho de autor. Algunas organizaciones pueden querer ampliar esta política aquí expresada, para incluir el permiso de copias para uso personal. La política también pudiera ampliarse para instruir a los trabajadores en el sentido de solicitar permiso antes de generar copias en exceso de la cantidad que pudiera ser considerada justo para su uso. La política, de manera deliberada, no hace mención de ninguna tecnología en particular, de modo que las copias se pudieran hacer con un computador personal o una máquina copiadora.

Políticas Relacionadas: “Derechos de Propiedad Intelectual”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

9. Revisión de los Convenios de Licencia del Software

Política: El convenio de licencia de todos los programas de computador debe ser revisado periódicamente.

Comentario: Esta política pondrá de manifiesto que una organización se preocupa por el cumplimiento de los convenios de licencia de software, si algún día la Empresa X fuere demandada por reproducción no autorizada. La verificación del cumplimiento de los convenios de licencia se automatiza cada día más, por ejemplo, como es el caso de redes de área local para programas de inventarios. Esos programas revisan automáticamente el hardware y software en cada computador personal (PC) o puesto de trabajo conectado en red. La existencia de una política semejante, puede también disuadir al usuario tentado a hacer copias no autorizadas. Algunas organizaciones tal vez prefieran limitar esta política a los PC y estaciones de trabajo, el ambiente de sistemas de menor escala donde tiene lugar la mayor parte del copiado sin autorización.

Políticas Relacionadas: “Copias Autorizadas de Software”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

10. Evidencia de Licencia de Software

Política: Cuando se adquieran sistemas en paquete, la fuente debe entregar evidencia escrita del software que se traspasa.

Comentario: Esta política esta dirigida, en primer lugar, a los departamentos de compras y adquisiciones, aunque también es pertinente para cualquier integrante del personal en funciones de compras de computadores y sistemas de comunicaciones. Las fuentes de sistemas empaquetados, tales como los fabricantes de equipos originales y revendedores de valor agregado, en ciertas instancias hacen copias no autorizadas del software. En ese proceso violan las licencias de derechos de autor. Aumentan los casos documentados de sistemas de computador personal con software instalado en el disco duro que se venden sin licencia apropiada. Las organizaciones deben obtener prueba escrita de que las licencias son legítimas para evitar la responsabilidad de violaciones de derechos de autor. Las garantías verbales del proveedor no son suficientes, ya que puede haber conflicto sobre lo que se dijo en el momento de la venta.

Políticas Relacionadas: “Avisos de Derechos de Autor en Software” y “Revisión de los Convenios de Licencia del Software”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

11. Copias Autorizadas de Software

Política: La gerencia debe hacer los arreglos apropiados con todos los proveedores de software para obtener copias licenciadas, cada vez que se requieran copias adicionales para las actividades del negocio.

Comentario: Esta política garantiza que la gerencia colocará los pedidos de copias adicionales del software necesario, en lugar de hacer copias no autorizadas. Los trabajadores con frecuencia insisten que fueron obligados a hacer copias adicionales no autorizadas porque la gerencia no suministró las mismas en cantidades suficientes. Esta política evita que tales posturas se conviertan en excusas para copiar software ilegalmente. Esta política puede ser útil para demostrar que la Empresa X tiene la intención de cumplir los convenios de licencia de software.

Políticas Relacionadas: “Revisión de los Convenios de Licencia del Software”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

12. Copias de Software

Política: El software de terceros en posesión de la Empresa X no deben ser copiado hasta que no se haga en conformidad con los convenios de licencia pertinentes de traspaso, y cuando la gerencia haya autorizado tal copiado con propósitos de planificación de contingencias.

Comentario: Esta política es particularmente pertinente en el caso de los computadores personales, estaciones de trabajo, servidores de redes de área local, sistemas cliente-servidor y otros sistemas de menor escala. Esto se debe a que es precisamente en el ambiente de los sistemas de menor escala donde ocurre con más frecuencia el copiado no autorizado. Esta política informa a los usuarios que todo copiado ha de ser consecuente con los convenios de licencia. La política también pone sobre aviso a los usuarios, que el copiado no puede ser permitido aunque sea consecuente con los

convenios de licencia., excepto cuando sea autorizado por la gerencia para propósitos de planificación de contingencias.

Políticas Relacionadas:“[Copias Maestras del Software](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

13. Información y Software No Autorizados

Política: Los administradores del sistema deben retirar la información de terceros que no haya sido autorizada para su uso, en concordancia con los derechos de autor o el software para el cual Empresa X no tiene autorización específica para almacenar o usar, salvo que los usuarios involucrados puedan demostrar autorización de los propietarios de los derechos de autor.

Comentario:Los trabajadores de algunas organizaciones descargan material registrado de foros electrónicos, servicios de base de datos en línea y otras fuentes públicas. En muchas instancias, el copiado no es autorizado y constituye una violación de las leyes de derechos intelectuales. Esta política tiene el propósito de informar a los usuarios que no deben almacenar estos materiales en los sistemas o en las redes de la Empresa X. La política sirve para reforzar la intención de la gerencia en el apoyo de los derechos intelectuales ajenos. La política conlleva implícito que los administradores, auditores internos y tal vez otros, tienen el derecho de explorar los directorios de archivos de los usuarios para identificar información y software no autorizados. A veces, la palabra "periódicamente" se puede insertar en la política, y en tal caso habrá un proceso regular de revisión de los directorios del usuario. La efectividad de este proceso de revisión puede ser frustrado con facilidad por los usuarios que utilizan medios de cifrado, y por ésta, y tal vez por otras razones, la Empresa X pudiera optar por prohibir el cifrado.

Políticas Relacionadas:“[Avisos Públicos Inadecuados](#)” y “[Remoción de Material Ofensivo](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

14. Protección Aplicable del Derecho de Autor

Política: Los trabajadores deben investigar la propiedad intelectual de todo el material que visualicen en Internet, antes de usarlo para cualquier propósito.

Comentario:Esta política evita que los trabajadores de Empresa X violen los derechos de propiedad intelectual de terceros. La Empresa X, mediante recordatorios a los usuarios sobre derechos de autor, también pueden protegerse, aunque parcialmente, contra demandas por daños y perjuicios asociados con los actos ilegales de sus trabajadores. Esta política no se limita a los datos y puede demostrar que la Empresa X de ninguna manera incita o apoya el copiado de software no autorizado.

Políticas Relacionadas:“[Información y Software No Autorizados](#)” y “[Copias No Autorizadas de Software y Datos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

15. Duplicación de Software

Política: Los usuarios no deben copiar en medios de almacenamiento, el software suministrado por la Empresa X, transferir tal software a otro computador o divulgar dicho software a terceras personas sin permiso escrito de la gerencia de Tecnología Informática.

Comentario:Esta política garantiza que los usuarios no harán cambios en la configuración de sus sistemas ni copias, transferencias, o divulgaciones que pudieran violar las licencias de software de los vendedores. La política puede ser útil en cuanto el control de la distribución del software desarrollado en casa. El software comercial ya existe que permite la automatización de cumplimiento forzoso, en el cual caso no habrá necesidad de política escrita. Pero hasta tanto ese software no sea de uso general, la política puede ser necesaria. Esta política no interfiere las actividades regulares del negocio, mientras se suministre el apoyo técnico adecuado. Cuando los usuarios deben proveer su propio apoyo técnico, esta política será problemática. Esta política funciona cuando los usuarios tienen la configuración de software pre-instalada que se adapte a sus necesidades, y cuando se les haya entregado una política por separado sobre la necesidad de usar software únicamente que se haya adoptado como norma.

Políticas Relacionadas:“[Avisos de Derechos de Autor en Software](#)” y “[Archivos Críticos de Respaldo](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

16. Copias No Autorizadas de Software y Datos

Política: Todos los usuarios de sistemas de la Empresa X o de internet deben abstenerse de hacer copias no autorizadas de software o de cualquier material con derechos de autor que no sea considerado de uso personal, sin el permiso del autor o de la editorial.

Comentario: Esta política tiene como propósito el designar con claridad la responsabilidad y la culpabilidad legal por el copiado de software y datos. Dado que no es factible que la gerencia supervise cada acto del trabajador, esta información pone sobre aviso al trabajador con respecto a los riesgos que corre por hacer copias no autorizadas. Esta política es importante en cuanto va más allá de la simple prohibición de hacer copias de software no autorizadas, ya que hace referencia específica a copias de material no autorizado tomado de Internet. Un ejemplo común viene representado por los gráficos usados en las páginas web. Muchos usuarios hurtan tales gráficos y los usan sin obtener la autorización del Propietario. La gerencia quizás no pueda ubicar los culpables de realizar las copias no autorizadas, por lo que se recomienda consultar con los asesores legales internos antes de adoptar una política como ésta.

Políticas Relacionadas: “Copias Maestras del Software” y “Revisión de los Convenios de Licencia del Software”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Material Con Derechos de Autor No Autorizado

Política: Los trabajadores no deben participar de ninguna manera ni en ninguna oportunidad en la distribución, transferencia o intercambio de copias ilegales de ningún material con derechos de autor.

Comentario: Esta política informa a los trabajadores que la Empresa X no tolerará ninguna actividad ilegal que involucre la reproducción no autorizada de material registrado como propiedad intelectual. La política es motivada por los sitios de Internet que suministran copias gratuitas pero ilegales de software, libros, música

y otros materiales, y que migran rápidamente a través de los sitios para evitar detección o acciones judiciales. La política también está motivada por los sitios que distribuyen los seriales necesarios para activar el software que no tiene protección contra copiado. Esta política prohíbe visitar, participar en el copiado o tomar copias de cualquiera de estos u otros sitios relacionados. La organización que adopte esta política aclara que no alienta la asociación del trabajador con estos sitios, lo cual demostrará que la organización no debe ser responsabilizada por cualquier daño sufrido por terceras personas, aún cuando los sistemas informáticos de la organización que formula la política los hubiese usado el trabajador involucrado.

Políticas Relacionadas: “Duplicación de Software” y “Directorios Modificables por el Público”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

18. Libros Electrónicos con Derecho de Autor

Política: Todos los libros electrónicos u otras obras con derechos de autor con base en textos publicados por la Empresa X en Internet o en cualquier otra red de acceso público, deben estar en mapas de bits.

Comentario: Esta política refleja la renuencia de las editoriales a la publicación de sus materiales registrados en Internet, y muchas temen legítimamente que tal forma de publicación conduzca rápidamente a la reproducción masiva no autorizada, y que como resultado pierdan sus derechos sobre la obra. Las editoriales han usado versiones de mapas de bits. El propósito de este enfoque es el de frustrar la piratería o el mal uso del material registrado, y dificultar el trabajo de los piratas de libros. Este enfoque, desafortunadamente, significa que el valor del material montado se degrada por no estar disponibles las búsquedas de palabras clave y otras funciones automáticas. Esta política será reemplazada con sistemas cifrados que controlarán la compra y distribución de información registrada en Internet.

Políticas Relacionadas: “Monitoreo en Internet del Uso de la Información” y “Material Con Derechos de Autor No Autorizado”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

19. Monitoreo en Internet del Uso de la Información

Política: El departamento Legal debe monitorear Internet por lo menos una vez al mes para detectar el uso no autorizado de las marcas registradas de la Empresa X, marcas de servicio, nombres de marca, o materiales registrados propiedad de la Empresa X.

Comentario: Esta política asigna la función de explorar Internet rutinariamente para garantizar que los derechos legales de la organización no han sido infringidos. Esto, además de controlar la infracción de la marca de fábrica y de los derechos de autor, puede incluir métodos para detectar declaraciones difamatorias contra la organización. La función pudiera ser ejercida por otros departamentos, pero el departamento Legal debe hacerles un seguimiento. Los servicios de terceros que ejercen esta función pueden utilizar software especial para automatizar buena parte del trabajo. Certo software del dominio público puede explorar la Internet para buscar materiales registrados, incluyendo los gráficos. Una motor de búsqueda se pueden usar para encontrar menciones de nombres, marcas de fabricas, y marcas de servicio. Algunas organizaciones pudieran tener interés en saber quién tiene enlaces a su sitio web. Las organizaciones deben tomar medidas para proteger sus derechos legales, o correr el riesgo, en algunas jurisdicciones, de perder sus derechos legales.

Políticas Relacionadas: “[Monitoreo de Mensajes de Correo Electrónico](#)” y “[Responsabilidad de Monitorear Contenido](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

20. Uso de Marcas Registradas de Terceros

Política: La página web y los sitios comerciales de la Empresa X no deben utilizar marcas registradas de otras organizaciones o marcas de servicio, excepto cuando el uso refleja los atributos verdaderos de los productos o servicios de la Empresa X, y cuando se haya obtenido permiso del asesor legal de la empresa.

Comentario: Esta política evita los problemas legales, la mala publicidad, y la tensión en las relaciones con los competidores, socios del negocio o con los proveedores. El uso de las marcas de fábrica de otras organizaciones o su marca se servicio se puede percibir como un artificio engañoso para atraer al público al sitio web propio, a través de motores de búsqueda. Esta política reconoce los derechos de terceras organizaciones a sus propias marcas de fábrica y marcas de servicio, y asume

una postura conservadora respecto del uso de esos conjuntos de caracteres. Esta política, más allá de evitar litigios, puede ayudar también en el mantenimiento de buenas relaciones con clientes en potencia, ya que las quejas se reducen a un mínimo.

Políticas Relacionadas: “[Propiedad Intelectual](#)” y “[Páginas Web No Oficiales](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

21. Acuerdos de Confidencialidad de Terceros

Política: Los trabajadores no deben firmar acuerdos de confidencialidad suministrados por terceras personas sin la previa autorización del asesor legal de la Empresa X, designado para manejar asuntos de propiedad intelectual.

Comentario: Los trabajadores pueden firmar acuerdos de confidencialidad con terceras personas, sin mayor preocupación, con el fin de acelerar las conversaciones con proveedores, clientes, y socios estratégicos en potencia. Con dicho procedimiento pueden obligar a su organización a pagar regalías, en el supuesto de que la organización pudiese mercadear, en un futuro, productos o servicios similares. También podrían, mediante dicho acuerdo de confidencialidad, impedir legalmente que la organización introduzca un producto o servicio similar. Para evitar estos y otros resultados desafortunados y perjudiciales, esta política requiere que todos los acuerdos de confidencialidad sean canalizados a través del asesor legal o el asesor externo autorizado.

Políticas Relacionadas: “[Acuerdos de Confidencialidad — Terceros](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

22. Revisión de Secretos Empresariales y Derechos de Autor

Política: El departamento Legal, en conjunción con la gerencia de Seguridad de Información, debe preparar una revisión anual de las leyes que protegen la propiedad intelectual y la información, que incluya el desarrollo de un inventario de los asuntos legales relativos a la información de la Empresa X, una evaluación de la eficiencia y efectividad de los controles

de estos asuntos, y una lista de cambios recomendados para su revisión y discusión subsiguientes en la comisión de administración de Seguridad informática.

Comentario: Esta política requiere que el departamento Legal y el departamento de Seguridad informática tomen conciencia de los asuntos legales asociados con la seguridad informática. Estos asuntos incluyen la violación de la marca de fábrica y de los servicios de marca, la violación de patentes, violación de derechos de autor y la violación de la privacidad. Los requisitos legales y regulatorios, en muchos casos, determinarán los requisitos de los sistemas informáticos. En muchas organizaciones los asuntos legales y regulatorios no se han explorado lo suficiente. Por lo tanto, estas organizaciones están en gran desventaja, porque a veces operan sin la orientación o asistencia externa adecuada. Esta política cambia el manejo de estos asuntos legales, de

reactivo a proactivo. Es necesario realizar una clara distinción entre este tipo de análisis legal y regulatorio, y la evaluación del riesgo en seguridad informática. Aunque algunos de estos asuntos pueden ser examinados en cada tipo de proyecto, los dos proyectos involucran metodologías diferentes, especialistas diferentes y tópicos diferentes. Nada de lo mencionado en la política implica que no se pueda utilizar un consultor externo o algún otro tipo de ayuda externa para este trabajo especializado

Políticas Relacionadas: “Evaluación de Riesgo de Seguridad Informática en Toda la Organización” y “Declaración de Secreto Industrial”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

12.01.03 Protección de los Registros Organizacionales

1. Información de Registro del Cliente

Política: Las personas que mantienen los registros que reflejan las actividades de un usuario o de las personas asistidas por computadores, deben eliminar la información que identifica a los usuarios o personas asistidas tan pronto termine la relación de la Empresa X con dichas personas.

Comentario: Esta política conserva la privacidad del individuo o persona asistida por computadores. Si la Empresa X ya no necesita la información contenida en los registros, entonces ésta debe ser eliminada de inmediato. Por ejemplo, tan pronto lo devuelva en buenas condiciones, una biblioteca eliminaría la identidad de quien haya tomado un libro en préstamo. Las palabras "tan pronto" pueden ser demasiado inmediatas para algunas organizaciones. Ellas pudieran preferir incluir las palabras "30 días a partir de..." Esta política no impide a la Empresa X mantener estadísticas relativas a la actividad del negocio. Sólo restringe el mantenimiento de información que permita llegar hasta los individuos. Una biblioteca podría mantener estadísticas relativas a los libros tomados en préstamos con más frecuencia, sin tener que mantener los datos acerca de los usuarios específicos que los tomaron en préstamo. La palabra "cliente" puede tener que modificarse para atender las necesidades de la organización. Las alternativas comunes incluyen "cliente", "paciente" y "usuario." Esta política podría ser modificada para reflejar el hecho de que ciertos registros tendrán que ser retenidos hasta tanto no se haya recibido el pago, las

cuentas hayan sido balanceadas, o se haya demostrado que la seguridad del sistema de computación es aceptable. Por ejemplo, pudiera ser necesario mantener los registros de actividad del usuario del computador durante tres meses. Un plazo semejante puede ser necesario para satisfacer a la gerencia en el sentido de que no se han cometido delitos de computación, caídas del sistema, o incidencias que requieran apoyo de los registros.

Políticas Relacionadas: “Divulgación del Registro de las Actividades del Cliente”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Retención de la Información Personal

Política: La información personal retenida en los sistemas informáticos de la Empresa X debe ser eliminada cuando la información ya no se necesite para la conducción del negocio y cuando ya no se necesite para el cumplimiento de requisitos legales o regulatorios.

Comentario: Esta política elimina información personal o privada tan pronto se considere innecesaria, evitando así el uso adicional con fines no autorizados. Esta política también elimina la divulgación que pudiera violar la privacidad de las personas descritas en los registros. La política es deliberadamente ambigua en cuanto a las palabras "ya no se necesite". Si la Empresa

X quisiera conservar las direcciones y números de teléfonos para avisos futuros relacionados con mejoras o actualizaciones del producto, se trataría de un propósito de negocios y, por lo tanto, estaría permitido por esta política. Esta política también tiene una segunda intención, la cual es mantener a un mínimo los registros de manera tal que se puedan manejar de forma económica y ordenada. La política también reduce los registros históricos que pudieran convertirse en blanco de procedimientos legales que buscan información incriminatoria para utilizarla en litigios judiciales.

Políticas Relacionadas: “[Información de Registro del Cliente](#)” y “[Período de Retención de la Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Destrucción de Registros de Transacciones

Política: La Empresa X debe destruir el registro de la transacción después de completar la transacción y después del plazo durante el cual se pueda aceptar una devolución.

Comentario: Esta política rutinariamente destruye la información que podría ser usada para comprometer la privacidad de los clientes, y es adecuada no sólo para el consumo interno, sino también para su liberación al público. La política reconoce que el almacenamiento en archivos de los registros de las transacciones introduce peligros graves a la confidencialidad. La oposición de la gerencia de Mercadeo puede hacerse sentir al adoptar esta política. Los especialistas en mercadeo insistirán que necesitan los registros de las transacciones para el almacén de datos, para la extracción de datos y para la generación de perfiles de clientes y poder ofrecer así un mejor servicio. Esta política probablemente será adoptada sólo por organizaciones concienzudas que verdaderamente creen en la necesidad de salvaguardar la privacidad de sus clientes, y que entienden que los perfiles de las transacciones representan un riesgo grave a la privacidad. Nada de lo contenido en esta política impide que una organización pueda recopilar estadísticas sobre cuáles productos se venden, o cuándo se compran, ya que toda tal información puede ser generada con base en estadísticas generalizadas. Cierta información contable debe retenerse para efectos de impuestos e informes financieros. Esta información puede vincularse al número de una tarjeta de crédito u otra información de pago, en lugar del nombre del cliente, el número de seguridad social u otros identificadores personales.

Políticas Relacionadas: “[Destrucción de Mensajes de Correo Electrónico](#)” y “[Enlaces Entre la Información Privada y la Identificadora](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

4. Retención de la Información Sensible

Política: Se debe establecer un período de retención para toda la información sensible.

Comentario: Esta política estimula el descarte de información sensible cuando deja de ser útil, y reduce las probabilidades de que llegue a manos de personas no autorizadas. La información puede estar clasificada como sensible al momento de ser destruida. El simple descarte, generalmente no es apropiado para la información sensible. Una política separada debería especificar el método de destrucción. Esta política facilita el descarte de la información en el momento apropiado, lo que a la vez reduce los costos de almacenamiento. La política puede ser modificada para insertar palabras que declaran que, en ausencia de una fecha específica para el descarte, se puede indicar la fecha para la toma de tal decisión. Si se ofrece esta opción, entonces pudieran ser necesarios el nombre y número de teléfono de contacto. Esta política supone la existencia de una política que defina el término “sensible”.

Políticas Relacionadas: “[Disposición de Información en Papel](#),” “[Clasificación de Datos en Cuatro Categorías](#),” “[Período de Retención de la Información](#),” y “[Cronograma de Retención de los Archivos Almacenados](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y altos

5. Identificación de Registros Vitales

Política: Los gerentes departamentales deben identificar y mantener una lista actualizada de los registros vitales que requieren sus departamentos para restaurar operaciones después de un desastre.

Comentario: Esta política tiene por intención la clara asignación de responsabilidades para la identificación y mantenimiento de la lista de registros vitales, llamados a veces registros esenciales. El hecho de que los gerentes de departamento han de preparar y mantener la lista, requiere que piensen sobre la información que necesitan sus departamentos. Esta lista se puede utilizar para la planificación de contingencias y para efectos de

respaldo. Algunas organizaciones pueden querer definir el significado de registros vitales de manera más concreta. Por ejemplo, hacer mención de la información necesaria para la transacción regular de negocios, restaurar la posición financiera y legal de la Empresa X, y conservar los derechos de la empresa, su personal y clientela. También puede ser necesaria la definición de desastre. En algunas organizaciones, el personal de planificación de contingencias distribuye un formulario, donde se hacen preguntas para orientar a los gerentes en la identificación de los registros vitales y la frecuencia de respaldo para esta información. Esta política sólo se distribuiría en términos generales entre los gerentes de departamentos.

Políticas Relacionadas: “Copias de Información Sensible, Crítica o Valiosa” y “Retención del Documento Fuente”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Almacenamiento de Registros Vitales

Política: Los registros de negocios vitales se deben mantener en cajas fuertes anti-incendios y cerradas cuando no estén en uso para propósitos del negocio.

Comentario: La intención de esta política no sólo es la de garantizar que la organización designe específicamente algunos registros vitales, sino también garantizar que los protejan contra incendios. Algunos de estos registros representan contratos de negocios, minutos de las reuniones de la junta directiva, informes para las distintas agencias gubernamentales y declaraciones del impuesto sobre la renta. Estas con frecuencia se encuentran en papel ya que requieren firmas autógrafas. El incendio es la causa más común de daños a los registros de papel, y esta política garantiza que los registros vitales del negocio estarán disponibles aunque las oficinas sean reducidas a cenizas. Algunas organizaciones pueden querer especificar el tipo de caja fuerte anti-incendios que ha de ser utilizada para estos efectos. El mantener estos registros en las instalaciones permite un grado adicional de control de acceso físico. Por ejemplo, las cajas fuertes pudieran estar ubicadas en un salón bajo llave.

Políticas Relacionadas: “Identificación de Registros Vitales” y “Destrucción de Información”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Medianos y altos

7. Período de Retención de la Información

Política: La información que no se encuentre específicamente en el Programa de Retención de Información, se debe retener sólo mientras sea necesaria.

Comentario: Esta política especifica los plazos de retención para varios tipos de información. La información está dividida de acuerdo con los tipos enumerados en el programa de retención. Por ejemplo, la información financiera, la impositiva y la médica estarán incluidas en el programa, pero no la información sobre inventarios en existencia de ciertos productos. Con frecuencia, el departamento Legal prepara una programación con base en las leyes y reglamentos locales. El aspecto atractivo de esta política es que los tipos de información pueden cambiar, pero no las palabras de la política. Esta política reconoce que la retención de información durante más tiempo del necesario, retrasa los procesos de recuperación de la información, y puede exponer a la Empresa X a problemas legales. Esta política podría ser modificada para que el lector sea referido al departamento de Administración de Registros o a la gerencia departamental en caso de que hubiere duda sobre el plazo apropiado. La política podría ser ampliada para permitir la prórroga del plazo de retención de la información en caso de que lo requieran procedimientos legales, si es necesaria una aprobación externa para el descarte o destrucción, o si la información pudiera coadyuvar al cobro de cuentas vencidas.

Políticas Relacionadas: “Cronograma de Retención de los Archivos Almacenados” y “Retención de la Información Sensible”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Cronograma de Retención de los Archivos Almacenados

Política: Todos los registros de contabilidad financiera, contabilidad de impuestos y documentos legales, deben ser retenidos durante un mínimo de siete años y el resto de los registros deben ser retenidos por un mínimo de cinco años.

Comentario: La política especifica de manera definitiva los parámetros de tiempo durante los cuales ciertos tipos de registros deben ser retenidos. Terminados los plazos, estos registros se pueden descartar sin violar la ley. Algunas organizaciones pudieran querer ampliar esta política para obligar a la destrucción de tales registros una vez terminado el plazo de retención. La destrucción

evitará que estos registros sean utilizados por la contraparte en un proceso legal por divulgación. La política puede también especificar los plazos para la información contenida en ciertos medios, tales como los mensajes de correo electrónico, y no sólo por el tipo de información. El asesor legal debería ser consultado para determinar los lapsos apropiados de la jurisdicción local, la industria y los contratos en vigor. Esta política hace uso de categorías amplias de información en su contenido para definir los varios requisitos de retención. El énfasis de esta política es en garantizar que la información se retenga por lo menos durante el período de tiempo especificado.

Políticas Relacionadas: “Período de Retención de la Información,” “Cronograma de Retención de Datos,” “Disposición de Información en Papel,” y “Manejo de Mensajes de Correo Electrónico”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

9. Cronograma de Retención de Datos

Política: Toda la información de la Empresa X debe ser resguardada de manera segura, de conformidad con el programa publicado por el departamento Legal.

Comentario:El único propósito de esta política es asignar en alguna persona la responsabilidad de fijar los plazos de retención de la información. El departamento Legal, por lo general, es el responsable, pero también pudiera serlo el departamento de Gerencia de Registros o el departamento de Seguridad Informática. Algunas organizaciones pueden ampliar el significado de las palabras "resguardada de manera segura" para aclarar dónde y cómo la información se debería almacenar. Estos requisitos de almacenamiento, por ejemplo, pueden variar de acuerdo con la sensibilidad, criticidad y valor de los datos.

Políticas Relacionadas:“Cronograma de Retención de los Archivos Almacenados” y “Período de Retención de la Información”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

10. Retención del Documento Fuente

Política: Los documentos fuente del negocio y los archivos electrónicos originales de entradas se deben retener hasta que las transacciones relacionadas se hayan completado, hasta que se haya realizado una

revisión gerencial de los documentos que integran estas transacciones, y durante un período de tiempo superior al que necesitarían tales transacciones para superar etapas contenciosas.

Comentario:El propósito de esta política es garantizar que el papel o el documento electrónico fuente no será destruido prematuramente. Un ejemplo de documento fuente lo constituye la solicitud que una persona presenta cuando busca empleo en una empresa. Cierta parte de esa información es introducida en el sistema computarizado y se convierte en un documento fuente. Es importante retener tal documento hasta tanto se complete la transacción, ya que muchas organizaciones no introducen en el computador toda la información que contiene el documento, y también porque con frecuencia se cometen errores de transcripción. La gerencia podría no tener suficiente información acerca del candidato como para tomar una decisión de empleo, y tendría que recurrir al documento original o solicitud para recabar más información. La revisión gerencial es necesaria para garantizar que la transacción se completó en concordancia con las intenciones de la gerencia. Este requisito permite que los documentos de origen sean utilizados en auditorías, como por ejemplo en la conciliación de registros contables. Esta política requiere un período de tiempo suficiente antes de descartar el documento, en previsión de cualquier disputa.

Políticas Relacionadas:“Período de Retención de la Información,” “Período de Retención del Documento Fuente,” y “Cronograma de Retención de los Archivos Almacenados”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

11. Período de Retención del Documento Fuente

Política: Los documentos fuente de negocios contenidos de datos de entrada se deben retener por un mínimo de 90 días, a partir de la fecha cuando la información fue ingresada en el sistema informático de la Empresa X.

Comentario:Esta política conserva la información original que puede ser importante en caso de problemas de computación o errores en la entrada de datos. Los documentos fuente retenidos también pueden ser de utilidad para efectos de control de calidad o de auditoría. El plazo de retención de 90 días es normal, y puede variar con base en las prácticas de la industria, la

naturaleza de la información que se maneja, las leyes y reglamentos locales y otras consideraciones. El asesor legal debe ser consultado sobre el particular. Esto le dará a la gerencia operativa una norma que puede usar para determinar el momento apropiado para la destrucción de documentos fuente, preferiblemente mediante máquina trituradora de papeles u otros medios seguros.

Políticas Relacionadas: “Retención del Documento Fuente” y “Cronograma de Retención de los Archivos Almacenados”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

12. Retención de los Datos de Transacciones con Aplicaciones

Política: Todos los datos de transacción de las aplicaciones deben ser mantenidas bajo protección hasta tanto se consolide el respaldo total de los archivos maestros de producción.

Comentario: Esta política especifica el tiempo mínimo absoluto para la retención de los datos de transacciones o de entrada. Después de este período de tiempo, el Propietario puede especificar requisitos adicionales de retención, lo cual puede incluir el almacenamiento fuera de sede. La justificación para el período mínimo absoluto de retención es que los datos de las transacciones con las aplicaciones se podrían usar como referencia en caso de que el programa de aplicación correspondiente colapsara o experimentara algún problema, exigiendo entonces la re-entrada de los datos. La política deliberadamente omite mención de los métodos de garantizar la protección de los datos de transacciones con aplicaciones. Los métodos específicos para lograrlo deberían ser determinados por el Propietario de la información, preferiblemente con el asesoramiento de un especialista interno de seguridad informática. Los términos "datos de transacciones" en algunos ambientes pueden ser sustituidos por "registros fuente".

Políticas Relacionadas: “Período de Retención del Documento Fuente” y “Respaldo Antes del Procesamiento”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

13. Destrucción de Información

Política: Toda la información de la Empresa X debe ser destruida o descartada cuando ya no se necesite.

Comentario: Esta política mantiene los registros de negocios a un mínimo y por ende elimina los innecesarios. A veces, el proceso se denomina purgar, y puede facilitar la eliminación de información que pudiera ser utilizada en perjuicio de la organización durante un proceso legal de divulgación. Un diccionario de datos podría ser un importante apéndice a esta política, porque puede ser utilizado para definir qué tipos de datos existen dentro de la organización, su ubicación, su antigüedad y cuáles controles se aplican a los datos.

Políticas Relacionadas: “Información Personal para el Funcionamiento del Negocio,” “Cronograma de Retención de los Archivos Almacenados,” “Directorio de Almacenamiento de Archivos,” “Información Sensible al Tiempo,” y “Disposición de Información en Papel”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

14. Destrucción de Registros

Política: Los trabajadores no deben destruir o descartar registros o la información de la Empresa X que sean potencialmente importantes, sin la previa autorización específica de la gerencia.

Comentario: Esta política informa a los trabajadores que no deben destruir o descartar información potencialmente importante, sin la previa autorización de la gerencia. Esta política debe ser acompañada con otras pautas que enumeren los plazos para la retención de los diferentes tipos de información. A menudo, esto se conoce como el programa de retención de datos. La política asigna a la gerencia la responsabilidad por la destrucción de registros e información, lo cual es aconsejable como manera de garantizar la supervisión de la gerencia en esta importante área. Esta política también constituye una técnica para evitar problemas si los registros son destruidos y luego la gerencia aduce ignorar las actividades descritas en los registros destruidos. Otra manera de manejar el problema objeto de esta política es la de restringir la cantidad de personas autorizadas para realizar la destrucción de los registros y la información.

Políticas Relacionadas: “Personal para Destrucción de Información”

Política Dirigida a:Todos

Ambientes de Seguridad:Todos

15. Cronograma de Destrucción de Registros

Política: Los trabajadores no deben destruir los registros de la Empresa X, a menos que éstos aparezcan en una lista de registros autorizados para la destrucción, o que puedan ser destruidos según las instrucciones que aparezcan en el Programa de Retención y Descarte de Registros.

Comentario: Esta política informa a los trabajadores que no pueden destruir los registros de la Empresa X, salvo cuando esté específicamente autorizado en documentos escritos. Sin tales instrucciones específicas, los trabajadores no los pueden destruir para ocultar actos no autorizados, o destruir inadvertidamente registros que posteriormente resulten de utilidad. Algunas organizaciones pueden optar por la ampliación de las excepciones mencionadas para incluir la autorización verbal por parte del archivista de la organización o del Propietario de la información. La lista de destrucción autorizada por lo regular incluye borradores que no se hayan puesto en circulación, copias preparadas para usos de corto plazo, material de referencia, publicaciones no actualizados, copias de respaldo innecesarias y formularios en blanco.

Políticas Relacionadas:“[Procedimientos para la Destrucción de la Información Sensible](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

16. Moratoria en Destrucción de Datos

Política: Al recibir la Empresa X una solicitud de descubrimiento electrónico, todas las actividades periódicas y organizadas para la destrucción de datos electrónicos deben detenerse inmediatamente hasta que el departamento Legal determine si las actividades de destrucción hacen peligrar tales datos buscados.

Comentario: Esta política informa a los administradores de sistemas, archivistas de datos, y a los operadores de computadores que deben estar prestos para detener los procesos normales de destrucción de datos inmediatamente, si reciben un aviso del departamento Legal. El proceso de descubrimiento involucra a la contraparte de una demanda judicial que solicita ciertos registros internos en posesión del demandado, y si el demandado permite de manera negligente que continúe el proceso

de destrucción de datos una vez recibido el aviso de descubrimiento, la organización puede ser objeto de sanciones legales, además de perjudicar la situación del demandado en el proceso. La política podría ampliarse para incluir otros tipos de solicitudes legales de información, como por ejemplo una citación legal. La existencia de una política como ésta, demuestra que la Empresa X tiene toda intención de cumplir plenamente con los requisitos legales. Algunas organizaciones pudieran ir más allá de los requisitos de la política con el establecimiento de un proceso formal para la notificación inmediata a todos los interesados que internamente estén involucrados en las actividades de destrucción periódica de datos. El usuario final que elimina información de su disco duro con el fin de liberar espacio no es actor en el proceso de destrucción de datos periódicos y organizados, y por lo tanto, no se ubica dentro del alcance de esta política. No obstante, éste debe ser avisado personalmente, en caso de que su computador personal pudiera contener alguna información buscada.

Políticas Relacionadas:“[Retención de la Información Personal](#)” y “[Destrucción de Mensajes de Correo Electrónico](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

17. Retención de Información Sensible para su Destrucción

Política: Los trabajadores no deben descartar información sensible en contenedores de basura de acceso público y deben retener la información sensible hasta que pueda ser programada su destrucción por métodos autorizados.

Comentario: Pudiera ser que los trabajadores, sin pensar, lo sencillamente descarten información sensible en sitios donde podría ser recuperada por espías industriales, hackers y otras personas interesadas. Esta política exige que los trabajadores retengan la información sensible hasta que puedan descartarla de manera apropiada. En ninguna parte de la política se mencionan copias en papel. Esta política se aplica a los discos flexibles y otros medios para capturar información sensible. Para que la política sea más comprensible para los lectores, se pudiera hacer mención específica de los diferentes medios en que se puede grabar información sensible. Esta política tiene en cuenta que muchos trabajadores se mantienen de viaje, alejados de la oficina donde pueden disponer de máquinas trituradoras de papel, desmagnetizadores, y

equipos de destrucción de información relacionados;. La política también es aplicable a los trabajadores ambulantes y teletrabajadores.

Políticas Relacionadas:“[Requisitos de Seguridad para Teletrabajo](#)” y “[Disposición de Información en Papel](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

18. Retención de la Información Sobre Violaciones y Problemas de Seguridad

Política: La información que describe todos los problemas de información de seguridad y violaciones debe ser retenida durante tres años.

Comentario:Esta política informa a la gerencia que no debe ser destruida cierta información importante relacionada con la seguridad. La información a que se refiere la política es de utilidad cuando se realizan evaluaciones de riesgo, cuando se planifican proyectos de seguridad informática y cuando se desarrollan presupuestos. También puede ser de utilidad en caso de demandas judiciales o medidas disciplinarias. Esta política es aplicable a las operaciones de registro del

computador y de correspondencia interna y a las notas provenientes de investigaciones secretas. La gerencia puede preferir que cierta información sea destruida con rapidez por temor que la desacredite. Algunas organizaciones pueden renunciar a esta política porque prefieren mantener la flexibilidad para destruir cierta información por temor a que ciertas personas en litigio contra la organización pudieran tener acceso la misma, y de esa manera sacar ventaja en los tribunales. Este temor se puede mitigar si se agrega la frase "a menos que se obtenga la aprobación previa de los asesores legales de la compañía". En apoyo a la noción de que la información que describe problemas de seguridad informática es valiosa, ciertos reglamentos gubernamentales ahora requieren que los problemas de seguridad sean participados a los entes regulatorios del gobierno. El ámbito de la política pudiera ser cambiada para hacer frente a los problemas y violaciones de la seguridad, y no sólo a lo relacionado con la seguridad informática.

Políticas Relacionadas:“[Análisis de Violaciones y Problemas](#)” y “[Reportes Externos de Violaciones](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

12.01.04 Protección de los Datos y Privacidad de la Información Personal

1. Efectos Personales y Comunicaciones Privadas

Política: Los trabajadores no deben introducir efectos personales a las instalaciones de la Empresa X o hacer uso de los sistemas de la Empresa X para comunicaciones personales sin entender que los mismos pueden ser revisados y monitoreados al azar.

Comentario:Esta política notifica a los trabajadores que corren un riesgo cuando introducen efectos personales a su puesto de trabajo o si entablan comunicaciones personales durante sus horas de trabajo. La política claramente define el lugar de trabajo como aquel constituido por un espacio público, y no de índole particular. La política es notablemente amigable en que instruye al trabajador en el sentido de mantener su privacidad, a la vez que refuerza la idea de que los sistemas informáticos de la Empresa X se deben utilizar únicamente para fines del negocio y el hecho de que los sistemas informáticos de la Empresa X pueden ser monitoreados. La política reconoce implícitamente que siempre habrá uso personal de los sistemas informáticos de la Empresa X. La política se puede utilizar como

defensa ante los alegatos de aquellos trabajadores que dicen haber sido objeto de espionaje de manera injusta o ilegal.

Políticas Relacionadas:“[Despidos Inmediatos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

2. Recopilación de Datos Personales Bajo Pretextos

Política: La Empresa X en ningún momento debe recopilar información personal con falsedades y declaraciones de pretexto relativas a su derecho a recibir tal información.

Comentario:Esta política garantiza a los clientes y prospectos que la Empresa X no se involucrará en prácticas no éticas que en algunas jurisdicciones pueden considerarse hasta ilegales. Esta práctica involucra el alegato de que una entidad tiene el derecho de recibir cierta información personal cuando, de hecho, dichas declaraciones son falsas. Por ejemplo, un investigador

privado puede acudir a un banco, identificarse como empleador y decir que quiere emplear a cierta persona; para luego preguntar si a tal persona le han devuelto cheques, ha incurrido en demoras de pagos o si ha manejado su cuenta de manera inaceptable. El banco, al creer que quien solicita la información tiene derecho a ella, la suministra. De modo que las declaraciones del investigador serían entonces solicitudes con pretexto. La política que se presenta aquí tiene por objeto asegurar a quienes lean una declaración de privacidad que la organización que adopta la política no se involucra en este tipo de comportamiento como medida para circunvenir las políticas de privacidad, los reglamentos o las leyes. La política sólo está orientada a los esfuerzos por obtener información personal, pero en ningún caso, para frustrar las solicitudes de terceros. Esto obedece a que casi siempre, la organización que posee la información privada no se pone a investigar los antecedentes del solicitante. Si la solicitud parece razonable, la información será suministrada.

Políticas Relacionadas: “[Uso de Investigadores](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

3. Renuncia a Derechos de Privacidad

Política: La Empresa X debe reservarse el derecho a revelar información confidencial a terceros con el propósito de cobrar cuentas pendientes, o de alguna manera forzar el cumplimiento de condiciones contractuales.

Comentario: Esta política aclara a terceros que puedan haber proporcionado información personal a la Empresa X, y a sus trabajadores internos, que existen límites al derecho de privacidad que haya publicado la organización. Por ejemplo, la Empresa X se puede ver obligada a comparecer en un tribunal para obligar a un cliente a pagar su cuenta, pero el proceso de comprobar los hechos en tribunal requiere la divulgación de información personal. La Empresa X no desea restringir su propia capacidad para cobrar cuentas, lo que requiere una política como ésta cuando se hayan adoptado otras garantías de privacidad. Los que se preocupan por el abuso de este derecho pudieran considerar la inclusión de términos en la política que describan el proceso con el cual se pueda verificar la legitimidad de una reclamación antes de revelar la información personal.

Políticas Relacionadas: “[Excepciones a las Políticas](#)” y “[Período de Retención de la Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

4. Divulgación de Información Privada

Política: Los registros de información privada se deben revelar únicamente al personal que se encuentre activamente involucrado de manera profesional con la persona o cuando la persona lo autorice por escrito.

Comentario: Esta política aclara cuándo es permisible la revelación de información privada, aun cuando la persona involucrada no haya dado su expreso consentimiento. Por ejemplo, si un paciente está hospitalizado y en coma, y por lo tanto incapacitado para dar su consentimiento, esta política permitirá a los médicos sin conocimientos previos del paciente, la revisión de su historia médica para poder asistirle con el tratamiento. Si bien es cierto que esta política es común en la industria de servicios médicos, también se puede adaptar a otras. Una compañía telefónica pudiera utilizarla para definir quién tiene acceso a los patrones de llamadas de los consumidores. La política es conveniente porque minimiza el papeleo asociado con el proceso de consentimiento, pero a la vez establece un grado mínimo de protección de la privacidad. La política también es conveniente porque permite a la organización revelar datos privados para proteger el bienestar de otras personas.

Políticas Relacionadas: “[Bloqueo de Divulgación de Información Privada](#)” y “[Uso del Registro Personal](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Recopilación de Información Privada

Política: Los trabajadores de la Empresa X y los sistemas informáticos no deben recopilar información privada, excepto con la previa autorización del departamento Legal de la empresa.

Comentario: El propósito de esta política es mantener a la organización emisora alejada de problemas relacionados con el campo de recopilación de información privada. Es mejor no tenerla, que tener que ocuparse de su protección; utilizándola sólo para fines aprobados y revelándola sólo a receptores autorizados. Este enfoque es particularmente conveniente para los comercios en Internet que operan en muchos países. En lugar de hacer seguimiento a todas las leyes pertinentes que rigen el manejo de información privada, esta política hace posible hacer caso omiso, pero seguro, de muchos de estos asuntos. Para muchos negocios que no requieren el

uso de información personal para sus actividades, es más económico y eficiente sencillamente prohibir la recopilación de tales datos. No es que la política prohíba la recolección de cualquier información privada para siempre, ya que es posible recoger información sobre origen racial, por ejemplo, si una agencia del gobierno requiere la compilación de un informe anti-discriminación.

Políticas Relacionadas: “[Información de Empleado Potencial](#)” y “[Restricciones en Contenido de Mensajes](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Low

6. Información Personal para el Funcionamiento del Negocio

Política: La Empresa X debe recopilar, procesar, almacenar y diseminar sólo la información que es necesaria para el funcionamiento correcto del negocio.

Comentario: Esta política se puede ampliar para prohibir la recopilación de información de las actividades personales de los empleados en horas fuera de la oficina que no afectan los asuntos del negocio. Esta política conserva los derechos de privacidad de los empleados, los clientes y otros que puedan tener relaciones con la organización, y simplifica los sistemas informáticos mediante la retención mínima de información. El alcance de esta política va más allá de los asuntos de privacidad, ya que tiene que ver con todo tipo de información. La política no provee pautas detalladas sobre cómo determinar si cierta información es necesaria. Esta es una omisión deliberada, porque el proceso de toma de decisiones y la información en que se basan dichas decisiones, pueden cambiar en el tiempo. El diccionario de datos de la organización también puede ser un suplemento importante para esta política.

Políticas Relacionadas: “[Inventario de Activos — Información](#)” y “[Destrucción de Información](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

7. Información Sobre Libertad de Expresión

Política: La Empresa X no debe recopilar información acerca de las opiniones sobre la libertad de expresión de los trabajadores.

Comentario: Esta política se puede ampliar para prohibir la recopilación de información acerca de las actividades personales realizadas fuera de la oficina que no afectan los asuntos del negocio. Si la gerencia recopila tales informaciones de expresiones y libertad de expresión, los trabajadores pueden desarrollar temor a expresarse libremente y a ser considerados adversarios de la gerencia. Esta política estimula la confianza hacia el empleador, porque respeta y quiere apoyar los derechos de sus empleados, como la privacidad. El término “trabajador” que se encuentra en la política se puede sustituir con variantes apropiadas, como “empleado”, “temporal” o “contratista”.

Políticas Relacionadas: “[Derecho a la Libre Expresión](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

8. Autorización de Recopilación de Información Privada

Política: La necesidad de tener la información debe ser documentada y aprobada por la Gerencia de Recursos Humanos, antes de que los trabajadores de la Empresa X recopilen información privada de los trabajadores, clientes u otras personas.

Comentario: Esta política está orientada a limitar la recopilación de información privada, lo cual reducirá la necesidad de establecer controles especiales para la protección de dicha información recién acumulada, y también evita indirectamente que la gerencia de la Empresa X mantenga una base de datos secreta de los empleados, o el establecimiento de sistemas encubiertos de supervisión del desempeño de los trabajadores. Originalmente destinada al uso del gobierno, esta política se aplica igualmente a organizaciones del sector privado interesadas en controlar el costo de la seguridad informática.

Políticas Relacionadas: “[Información Sobre el Monitoreo del Desempeño](#)” e “[Índices de Base de Datos Que Contienen Información Privada](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

9. Recopilación de Datos Privados

Política: La recopilación de información privada por los trabajadores de la Empresa X debe ser realizada a través de medios legales, y sólo con propósitos relacionados con las actividades de la Empresa X.

Comentario: Esta política proyecta la imagen de una organización preocupada por la privacidad, cuando en realidad no lo está. Esta política es un truco de relaciones públicas en lugar de ser un control sustancial que de verdad mejora la privacidad de las personas. La política no obliga a la organización emisora a nada serio, a menos que se vea obligada a lograrlo. La política facilita un medio para despedir al empleado que viole los límites fijados, pero que de todas maneras pudo haber sido despedido por otras razones. Esta política se incluye por ser de común, y para que se pueda comparar con otras políticas que sí tienen sentido. Esta política no se incluye en este libro porque sea recomendada.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” e “[Información Personal para el Funcionamiento del Negocio](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Recopilación Furtiva de Información Privada

Política: Los sistemas de computación y comunicaciones no deben recopilar datos privados de clientes o clientes potenciales, sin antes haber logrado un consentimiento claro y sin ambigüedades.

Comentario: Esta política mejora la imagen de la Empresa X y la lealtad de sus clientes. Al prohibir la recopilación clandestina de datos privados, los clientes y clientes potenciales se sienten más confiados al tener toda la información sobre el manejo de información privada de la Empresa X. Un ejemplo involucra la identificación automática de números (ANI, por sus siglas en inglés), o la identificación de la persona que llama. ANI capta los números de teléfonos de los que llaman sin el consentimiento del cliente potencial o existente. Algunas organizaciones hacen uso de esta información para llamadas de telemarketing, y otras pueden vender la información sin el consentimiento de la persona que llama. Esta política prohíbe la recopilación de la información ANI sin el consentimiento de quien llama. Esta política es una manifestación de un concepto más amplio, en el sentido de que la persona debería ser Propietaria de la información que la perfila.

Políticas Relacionadas: “[Herramientas de Monitoreo de Sistemas](#),” “[Áreas de Monitoreo Electrónico](#),” “[Uso de Tecnología Telefónica para Conferencias o Grabación](#),” y “[Recopilación de Información Privada](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

11. Consentimiento para la Recopilación de Información Privada

Política: La Empresa X debe obtener el consentimiento por escrito de los clientes antes de registrar cualquier información acerca de los mismos en un sistema informático computarizado.

Comentario: Esta política asume una postura pro-privacidad al no permitir que la información del cliente sea ingresada a un sistema computarizado, a menos que el cliente haya dado específicamente su consentimiento por escrito. Esta política apunta a las campañas de mercadeo, tales como las de correo directo o las llamadas de telemarketing a personas de un tipo específico. Algunas organizaciones piensan que estas restricciones a sus actividades de mercadeo son inaceptables, y que no deben adoptar esta política excepto cuando sea impuesta por ley. La política permite el uso de registros en papel mientras se consigue el consentimiento del cliente. Si las organizaciones que adopten la política pertenecen al sector salud, deben reemplazar el nombre de “cliente” por el de “paciente”.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” y “[Recopilación de Información Privada](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

12. Aviso de Recopilación de Información

Política: En cada instancia que se recopile información que identifique a una persona, se debe entregar en el momento y en el lugar de recopilación, una notificación explícita y entendible.

Comentario: Esta política sirve para aclarar cuándo y dónde se debe entregar una notificación sobre la recopilación de información. Esta política pone gran énfasis sobre la recopilación de información que identifica a las personas, tal como una dirección de correo electrónico, y requiere que todos los sitios de internet donde se esté realizando tal recopilación sean identificados como tal, sin consideración del conocimiento de usuario o su participación en el proceso de recopilación. Si las direcciones electrónicas fuesen recolectadas automáticamente de los usuarios que exploran las páginas web cuando las visitan, el hecho tendría que ser divulgado. De menos preocupación es aquella información que no identifica a la persona. Dado que

esta última no se relaciona con ninguna persona en particular, el potencial de abuso es bastante reducido, y ello se refleja en la ausencia de la necesidad de notificar. Algunas organizaciones pudieran querer hacer mención de una excepción, cuando la información privada pueda ser recolectada en secreto, como durante una investigación de un supuesto delito o de una actividad supuestamente abusiva.

Políticas Relacionadas:“Actividad de Monitoreo y Grabación” y “Anonimato del Cliente”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

13. Recopilación de Información Personal de Menores

Política: Información personal acerca de niños no debe ser recopilada por ninguno de los sistemas informáticos de la Empresa X, sin el consentimiento claro y sin ambigüedades de los padres o representantes.

Comentario:Esta política pone sobre aviso al personal técnico en el sentido de que no debe recolectar información personal de niños sin el consentimiento de los padres o representantes. Cómo obtener dicho consentimiento se omite deliberadamente en esta política. Lo ideal sería conseguir este consentimiento a través de un correo electrónico firmado digitalmente por uno de los padres que se pudiera verificar con un certificado digital. Esto puede consumir mucho tiempo, de modo que debe buscarse otra manera más eficaz. Por ejemplo, el suministro de una tarjeta de crédito válida, por lo regular se considera evidencia suficiente de que se es adulto. Esta política se sugiere por el aumento del uso de Internet para recolectar información personal de las personas, particularmente de niños. Los niños no tienen la sofisticación para proteger su propia privacidad, de modo que son los padres los llamados a cumplir esa responsabilidad. La política no especifica que tiene que ser en Internet, ya que tal información se puede conseguir por otros medios, por ejemplo, por teléfono. Esta política también establece que la Empresa X es consciente. Esta política con algunas modificaciones se puede publicar en la página web. La política de manera deliberada no declara sobre cómo se recopila la información. Pudiera ser solicitada específicamente a través del registro de entrada de usuario y un formulario web, o se pudiera lograr automáticamente a través de software de registro de la actividad del usuario.

Políticas Relacionadas:“Acceso a Material Adulto” y “Autorización para Inclusión en Sistemas de Datos Privados”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

14. Distribución de la Información Personal

Política: El acceso a cualquier recopilación de información personal de clientes potenciales y otros con quienes la Empresa X tiene relaciones comerciales, debe ser estrictamente controlada con base en la necesidad de conocer, y sin el debido consentimiento la información no se debe vender, intercambiar o distribuir a terceros.

Comentario:Esta política permite la recopilación de cierta información con propósitos comerciales, y conserva la privacidad de la persona al no permitir que sea distribuida a terceros. La distribución no autorizada a terceros es una manera de garantizar que la información no será utilizada de otra manera ajena a la voluntad de la persona. La política permite que la información sea usada para propósitos internos, inclusive los diferentes a la intención original. Esto permitiría, por ejemplo, el minar datos cuando se descubran nuevas relaciones entre varios grupos de datos de la clientela. Esta política no requiere que la persona convenga por adelantado la recopilación de información, pero pudiera ser una transacción aceptable para algunas categorías de negocios. Otros pueden creer que esta política concede a la persona derechos adicionales sobre su información. Estos negocios querrán intercambiar listas de direcciones y otras colecciones de información personal sin comunicarse con los clientes. Algunas pueden querer que se especifique la necesidad de consentimiento al tratarse de ciertos tipos de información, pero no para otros tipos. La política no infiere que la información personal requerida por ley tenga que pasar por el proceso del consentimiento. Algunas organizaciones pueden preferir especificarlo en la política.

Políticas Relacionadas:“Recopilación Furtiva de Información Privada”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

15. Recopilación de Información de Clientes

Política: Los procedimientos de soporte computarizado de la Empresa X no deben imponer la condición de suministrar información personal innecesaria para completar una transacción o para proveer productos o servicios.

Comentario: Esta política tiene el propósito de simplificar las transacciones y permitir al cliente decidir si suministra cierta información personal. La notificación de que cierta información personal es opcional puede ser agregada a ciertos formularios, o puede ser suministrado por teléfono cuando se recaba la información personal. Algunas organizaciones pueden preferir la mención de la necesidad en la política. Por ejemplo, un cliente que envía la tarjeta de registro de garantía del producto, sencillamente no contesta la pregunta referente a sus ingresos, y el proceso de registro se realiza sin tal información. Esta política no hace mención de la solicitud de cierta información personal, pero sí menciona que esta información jamás será requerida. La investigación de mercado y otros esfuerzos para comprender al consumidor no serán impedidos, y trampoco interfiere con la recopilación de información personal necesaria, tal como el número del seguro social para ciertos requisitos del impuesto sobre la renta.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

16. Métodos de Recopilación de Información Privada

Política: La Empresa X debe emplear los métodos menos intrusivos a su disposición para recolectar información confidencial de sus clientes, prospectos, empleados, y otros asociados con su organización.

Comentario: Esta política tiene el propósito de garantizar a los clientes, prospectos, empleados y otros, que la organización emisora trata por todos los medios de reducir a un mínimo la carga de recopilación de información. Una declaración semejante pudiera ser útil para propósitos de mercadeo al brindar otro incentivo para hacer negocios con la organización emisora. Esta política supone que la organización emisora goza de un registro integrado de clientes, en lugar de una base de datos aislados que sirven diferentes propósitos.

Políticas Relacionadas: “[Recopilación Furtiva de Información Privada](#)” y “[Recopilación de Información de Clientes](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Captura de Información Biométrica

Política: La información personal biométrica no debe ser captada por ninguno de los sistemas de la Empresa X, excepto cuando la persona descrita haya sido previamente notificada y haya acordado su captación.

Comentario: Esta política evita la captación furtiva de información biométrica personal que posteriormente pudiera ser usada para cometer fraude o violar la privacidad de la persona descrita en la información. Un fraude pudiera ocurrir si la información fuera incorporada en una licencia para conducir u otro dispositivo de identificación falso. La violación de la privacidad pudiera ocurrir si la información biométrica fuera utilizada para hacerse pasar por la persona para poder obtener información que de otra manera hubiera sido imposible. La recopilación encubierta de información biométrica pudiera también constituir un grave problema de imagen si a la poste fuera revelado que tal información se recabó sin el conocimiento o el consentimiento de la persona. Esta política supone que existen fuertes mecanismos de control para proteger la información biométrica. Esta política podría ser modificada para reconocer específicamente una excepción que involucre la investigación de supuestas actividades criminales. Esta excepción no se incluyó en la política sugerida porque el proceso de captación de datos, con frecuencia está bajo el control de cuerpos policiales, y no de los sistemas informáticos de la Empresa X.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” e “[Identificación Positiva para Uso del Sistema](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

18. Transferencia de Información Biométrica

Política: Los trabajadores no deben suministrar información biométrica a terceros excepto por requisito de ley.

Comentario: Esta política garantiza a las personas que utilizan sistemas biométricos que sus datos no serán revelados a terceros. Esta información debería ser de

particular preocupación para toda persona que esté registrada en un sistema biométrico, ya que tales datos personales pudieran ser utilizados para apoderarse de su identidad. Por ejemplo, los datos de sus huellas digitales pudieran ser utilizados para realizar un proceso de identificación en línea, y si un ladrón tiene los datos de otra persona, éste puede hacerse pasar por esa otra persona. Los datos biométricos también se pueden utilizar para propósitos diferentes a los que el usuario convino cuando se registró en el sistema biométrico. Esta política garantiza a aquellos que piensan registrarse en un sistema biométrico que no existen segundas intenciones. La organización que esté recolectando este tipo especial de datos personales podría usarlos en nuevas formas, pero el riesgo de usos no autorizados se reduce considerablemente si la información no se comparte con terceros.

Políticas Relacionadas: “[Captura de Información Biométrica](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

19. Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización

Política: La gerencia de la Empresa X debe notificar a todos los usuarios del sistema informático que en cualquier momento y sin previo aviso, la Empresa X puede examinar el correo electrónico archivado, los directorios de archivos personales, los archivos del disco duro y otra información almacenada en los sistemas informáticos de la Empresa X.

Comentario: Esta política informa a los usuarios de computadores que la información que almacenan, transmiten o de alguna manera procesan a través de los sistemas informáticos de la Empresa X, está sujeta a la revisión de la gerencia. Esto los instará a usar los sistemas informáticos sólo para propósitos del negocio. También ayudará a disuadir actividades no éticas o ilegales. Esta política es particularmente pro-supervisión en lugar de pro-privacidad, pero por lo menos define las expectativas que deben tener los trabajadores.

Políticas Relacionadas: “[Privacidad en Correo Electrónico](#),” “[Revisión de la Información Respaldada](#),” y “[Privacidad del Archivo Personal](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

20. Conducta de los Empleados Fuera de la Oficina

Política: La gerencia no debe entrometerse en la vida de los empleados o de alguna manera buscar manejar su comportamiento fuera de la jornada laboral, excepto cuando éste perjudique la capacidad del empleado para la realización de sus tareas de trabajo normales, o si afecta la reputación de la Empresa X de manera significativa.

Comentario: El propósito de esta política es restringir a la intrusión de la gerencia en la vida de los empleados. Ciertos eventos, tales como la estadía del empleado en una clínica y las circunstancias de su hospitalización, deberían ser discutidas con el gerente del empleado. Las relaciones afectivas entre compañeros de trabajo también deben ser discutidas porque podrían afectar el desempeño del empleado. La política también se puede utilizar para disuadir el comportamiento que puede conducir a demandas por acoso sexual o por invasión de la privacidad.

Políticas Relacionadas: “[Derechos de Propiedad Intelectual](#)” e “[Información de Empleado Potencial](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

21. Sistemas Secretos

Política: Con excepción de las investigaciones criminalísticas, no debe existir un sistema de registros personales en la Empresa X, cuya existencia sea desconocida para las personas descritas en el mismo.

Comentario: Esta política prohíbe la existencia de bases de datos secretos que puedan mantener los supervisores u otros como método de perseguir, hostigar, intimidar, o de alguna manera controlar a los empleados. La política desarrolla la confianza del trabajador en el sentido de conocer bien todos los sistemas utilizados para evaluar su desempeño y las perspectivas de ser promovidos. El propósito de esta política es también garantizar que todos los sistemas que contengan información del desempeño del personal sean del conocimiento, no sólo de las personas, sino también del personal de seguridad de informática. Si conocen la existencia de estos sistemas, estarán en mejores condiciones de garantizar la incorporación de medidas de seguridad apropiadas. La política también es aconsejable porque requiere la divulgación de todos los datos personales que luego pudieran ser incluidos en un diccionario de datos o directorio de datos. Esto ayudaría en los esfuerzos por estandarizar, categorizar y racionalizar los diferentes

tipos de información a lo largo de la organización. La excepción de la investigación criminalística se hace necesaria porque sería contraproducente informar a un supuesto delincuente de que una investigación está en proceso.

Políticas Relacionadas: “Inventario de Activos — Información” y “Herramientas de Monitoreo de Sistemas”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

22. Acceso a la Información Personal

Política: Cada persona, al solicitarlo por escrito, debe tener acceso a los registros de la Empresa X que contengan información personal referente a su vida personal o su condición.

Comentario: Muchas empresas conceden a los empleados el derecho de revisar periódicamente la información contenida en su expediente. Esta política le da a la persona el derecho de conocer la información que se ha utilizado para tomar decisiones que la afecten. El conocimiento de esta información por lo tanto, permite a las personas objetar o corregir las inexactitudes o declaraciones falseadas que aparezcan en el expediente. La política no expresa nada que obligue a la organización a divulgar detalles que no se relacionan con él, y estos detalles se pueden ocultar antes de la divulgación del expediente a la persona. La política permite que la gerencia revise el expediente para garantizar que sólo la información directamente pertinente a la persona se divulga. Algunas organizaciones permiten que sus empleados inserten breves comentarios en su expediente personal, en el evento de que la gerencia haya recibido alguna queja sobre inexactitudes o falsedades de información, pero decide no alterar la información contenida en el expediente de la persona. Esta política, de manera indirecta, se convierte en política de integridad de la información.

Políticas Relacionadas: “Declaración Explicativa del Empleado,” “Información Personal Incorrecta,” “Revisión del Archivo del Empleado,” “Distribución de los Registros del Personal,” y “Acceso al Archivo del Personal”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

23. Divulgación de Información Privada a Terceros

Política: La divulgación de información de los trabajadores de la Empresa X a terceras personas no debe ocurrir, salvo por mandato de ley, o con el consentimiento explícito e inequívoco del trabajador.

Comentario: Esta política evita demandas por invasión de la privacidad, difamación de carácter, difamación y calumnia. El propósito de esta política es garantizar que terceras personas no tengan acceso a la información confidencial de los trabajadores. Las únicas excepciones son cuando sea requerida por ley específicamente, como lo sería el caso de una citación judicial, o cuando la persona expresamente autoriza la transferencia, como lo sería el caso de información a ser utilizada por un empleador que investiga antecedentes. Por esta razón, y sin mayor autorización del trabajador, el empleador divulga sólo el hecho de que la persona ha trabajado o trabaja en la organización, el último puesto de trabajo, las fechas de empleo, y posiblemente si el trabajador sería re-enganchado. Algunas organizaciones divulgan sólo algunas partes de este tipo de información. Los ejemplos de tipos de información que no se divulgarian deben acompañar la explicación de esta política. Por ejemplo, la razón del retiro por lo general no se declara porque pudiera terminar en demanda por difamación. Esta política implica que acreedores, abogados, agencias de detectives privados y otros que busquen información que no sea relacionada con el trabajo, no la recibirán sin el consentimiento del trabajador.

Políticas Relacionadas: “Divulgación de Razón de Cese de Relación Laboral” y “Divulgación de Información a las Autoridades”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

24. Transferencia de Datos Privados

Política: La Empresa X sólo debe divulgar datos privados a organizaciones de terceros que se comprometan por escrito a mantener la información con un nivel adecuado de protección según lo determinado por la gerencia de Seguridad Informática.

Comentario: Esta política evita la divulgación a esas organizaciones de terceros que no se comprometan a proteger la información privada de manera adecuada. El tipo de divulgación a que se refiere esta política es aquel seleccionado por la organización que posee los datos, y no por la persona descrita en los datos. Esta política refleja una práctica de uso común en la cual se venden

listas para uso de una sola vez, el uso se especifica por adelantado y no se permiten usos subsiguientes. A la vez que estos contratos de listas para alquiler protegen los derechos de la organización a los datos, preservan la privacidad de las personas involucradas porque cada utilización queda definida y limitada. La política identifica a la gerencia de Seguridad de Informática como el único árbitro para determinar si procede su divulgación, ya que los requisitos específicos pueden cambiar en el tiempo y por jurisdicción.

Políticas Relacionadas: “Términos y Condiciones para el Acceso de Terceros” y “Diseminación de la Información”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

25. Registros de Divulgación de Información Privada — Detalles

Política: Los trabajadores de la Empresa X que divulguen información confidencial a terceros deben mantener registros de todas las divulgaciones, incluyendo la naturaleza de la información, a quien se divulgó y la fecha de tal divulgación.

Comentario: Esta política protege a la organización contra acusaciones injustificadas de invasión de la privacidad. Ciertas personas pueden acusar a una organización de haber divulgado información personal que los afecte. La organización, al no contar con los registros descritos en la política, tendría dificultades al tratar de comprobar que tal información no ha sido divulgada. Además, la política tiene como propósito apoyar a las personas en la investigación y acción contra el robo de identidad. Con estos registros de divulgación, se puede acumular una lista inicial de sospechosos. También, estos registros se pueden utilizar por personas empeñadas en corregir los errores que hayan sido propagados a través de múltiples bases de datos o múltiples organizaciones.

Políticas Relacionadas: “Uso de la Información Personal para Nuevos Propósitos,” “Divulgación de Receptor de Información del Cliente,” y “Notificación al Cliente de Solicituds de Registros”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

26. Transferencia Internacional de Información Privada

Política: No se debe realizar ninguna transferencia de información privada a otros países, sin importar la tecnología empleada, a menos que se tenga la autorización de la gerencia de Seguridad Informática, cuando la persona afectada está, o será destinada a cualquier país, o cuando la persona haya solicitado específicamente tal transferencia.

Comentario: Esta política evita que la información privada sea transferida de una jurisdicción altamente regulada a otra menos regulada. Sin los impedimentos a este flujo de información, los negocios tenderían a transferir información a sitios de costos menores y posiblemente frustrar la intención de las leyes y los reglamentos de privacidad. Esta política evita el desarrollo de ubicaciones donde los negocios puedan hacer lo que quieran en un ambiente sin restricciones. Cuando una organización adopta esta política demuestra su seriedad en materia de privacidad y que tiene el propósito de evitar el movimiento de datos privados que tengan fines de frustrar el amparo de la ley.

Políticas Relacionadas: “Transferencia de Datos Privados” y “Compromiso en Acuerdos de Confidencialidad”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

27. Bloqueo de Divulgación de Información Privada

Política: La Empresa X debe informar a las personas por anticipado que los datos personales en su posesión han sido solicitados por terceros, a menos que sea obligada a divulgarlos por mandato claro y autorizado por ley o reglamento, y a esas personas se les debe dar un plazo razonable de varias semanas para que tengan la oportunidad de cerrar el paso a dicha divulgación.

Comentario: Esta política evita futuros conflictos cuando una persona se queja de que la Empresa X debió obtener su autorización antes de divulgar ciertos datos personales. Esta política es oportuna, pero brinda cierta protección a la privacidad, y su implementación puede requerir acuse de recibo que indique que el solicitante, de hecho, recibió la notificación acerca de la divulgación. Esta política ofrece una flexibilidad para otros usos de la información, tales como el mercadeo en cruce de otros productos y servicios, en la suposición de que los productos son ofrecidos por la misma organización. Esta política establece que la persona afectada está

en control de la información personal, y es aplicable a una gran variedad de información personal, inclusive las libretas de direcciones domiciliadas en computador y calendarios de citas, así como a información personal, tales como las historias médicas.

Políticas Relacionadas: “Consentimiento para Acciones Cuestionables en los Sistemas”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

28. Divulgación de Información de Contacto de Trabajadores

Política: La Empresa X no debe divulgar los nombres, cargos, números de teléfono, ubicaciones, u otra información de contacto de sus trabajadores, excepto cuando sea requerido por razones de trabajo, mandato de ley, o cuando la persona haya autorizado su divulgación con claridad.

Comentario: Esta política protege la privacidad del trabajador, pero un efecto colateral de esta política es que el ritmo de los negocios se hace más difícil para los clientes, consumidores y otros que tengan la necesidad legítima de acceso a la información. Muchos telemarca-deres llaman a las organizaciones para preguntar el nombre de una persona en un cargo en particular, tal como el director de Mercadeo, para luego pedir ser comunicados con él. El director de Mercadeo luego está sometido a una promoción de ventas que no quiere escuchar. Esta política debe evitar estas llamadas. Las recepcionistas y operadores de centrales telefónicas deben indicar a los solicitantes que envíen el material por correo dirigido al "Director de Mercadeo", o cualquier otra que sea el blanco, para garantizar que la organización no pierda información importante. Esta política no está orientada a la información tal como el sueldo del trabajador, sólo a información de contacto. En términos generales, es aconsejable que las recepcionistas, operadores de teléfonos, personal de vigilancia, y otras personas que tengan contacto significativo con el público, reciban instrucciones específicas acerca de la información interna que puedan divulgar.

Políticas Relacionadas: “Divulgación de Información Privada a Terceros”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

29. Divulgación de Razón de Cese de Relación Laboral

Política: La razón del cese de la relación laboral de los trabajadores no debe ser divulgada a terceras personas, excepto con autorización previa de un alto funcionario de la Empresa X o cuando la divulgación se hace por mandato de ley.

Comentario: Esta política, más allá de proteger la privacidad del empleado afectado, previene las demandas por difamación, calumnia y similares. Algunas organizaciones pueden preferir no divulgar esta intención adicional en la redacción de la política, mientras que otras no desean ser tan explícitas. En algunas jurisdicciones, un antiguo empleador pudiera ser declarado en negligencia si la razón del cese laboral obedece a un comportamiento criminal, si el ex-empleado repite ese comportamiento en el próximo sitio de trabajo. Esta situación se puede sumar como otra excepción. Esta política se puede estrechar para excluir a quien no tenga necesidad de conocer la información. Otros trabajadores que por lo regular no tenían interacción laboral con un empleado retirado, no se enteraban del hecho. Esta estrechez del alcance reduce aún más los riesgos de demandas por difamación, calumnia y similares.

Políticas Relacionadas: “Divulgación de Información Privada a Terceros” y “Divulgación de Cambio de Situación”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

30. Divulgación de Cambio de Situación

Política: La información detallada del cambio de situación de un trabajador es estrictamente confidencial, y no se puede divulgar a ninguna persona, excepto a quienes tienen legítimo derecho de conocerla.

Comentario: Esta política evita que las personas de la gerencia de Recursos Humanos y otros que sean partícipes de la información sobre los cambios de situación se lo divulguen a terceros que no tienen porqué saberlo. Si bien es cierto que el hecho de un cambio de situación típicamente sería comunicado a recepcionistas, personal de vigilancia del edificio, personal de gerencia de seguridad y administradores de seguridad informática, los motivos del cambio no deben ser comunicados a estas personas. Si se divulga a quienes no tienen porqué saberlo, la persona involu-

crada en el cambio puede alegar difamación de carácter o invasión de su privacidad, lo que pudiera desembocar en demandas o en actos vengativos.

Políticas Relacionadas: “Divulgación de Razón de Cese de Relación Laboral”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

31. Acceso a Divulgación de Registros de Datos Privados

Política: Los trabajadores deben recibir acceso a los registros que reflejen la divulgación de su propia información privada, y se les debe dar suficiente información para que ellos puedan comunicarse para corregir errores o suministrar información adicional.

Comentario: Los trabajadores deben tener la oportunidad de suministrar su propia interpretación de los eventos, si ello fuera diferente a lo plasmado en los registros de la Empresa X. Esta política permite a los trabajadores corregir lo que consideren inexacto o información falseada cuando la Empresa X opta por no tomar ninguna acción al respecto. La política se pudiera modificar para declarar que los trabajadores recibirán esta información sólo cuando la Empresa X decida no alterar un registro privado de la manera solicitada por los trabajadores afectados.

Políticas Relacionadas: “Registros de Divulgación de Información Privada — Mantenimiento”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

32. Información Sobre Desempeño del Trabajador

Política: La información del desempeño del trabajador no se debe suministrar a otros que no tengan la necesidad legítima de conocerla, relacionada con el negocio.

Comentario: Esta política tiene el propósito de evitar que el trabajador se sienta humillado, hostigado, acosado porque su desempeño se haya hecho público. En muchas ocasiones, los compañeros de trabajo tendrán idea general del mismo y no los toma por sorpresa. Esta política no interfiere del derecho de la gerencia a disciplinar al empleado o cesarlo con base en un bajo desempeño. La política puede fomentar la opinión positiva de los empleados con relación a los

propósitos de la gerencia y el alcance del interés de la organización por el bienestar del empleado. Esta política también puede ser útil para que la empresa evite problemas relacionados con las leyes y reglamentos sobre la privacidad.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

33. Privacidad del Archivo Personal

Política: Los expedientes personales en los computadores de la Empresa X y en los escritorios de los trabajadores de la Empresa X se deben manejar como para garantizar que otros trabajadores, inclusive los gerentes y los administradores de sistemas, no los puedan leer, salvo que tal acción sea parte de una investigación iniciada por Seguridad Informática, o un intento por descartar o reubicar los expedientes después del retiro del trabajador de la Empresa X.

Comentario: Esta política aclara las expectativas de la confidencialidad de los expedientes personales de los trabajadores, y requiere que los mismos no sean leídos por otros trabajadores, inclusive los gerentes y administradores del sistema. La política se puede modificar para hacer mención específica del correo electrónico, computador personal y archivos de las estaciones de trabajo.

Políticas Relacionadas: “Examen de los Datos Almacenados en los Sistemas” y “Privacidad en Correo Electrónico”

Política Dirigida a: Todos

Ambientes de Seguridad: Bajos y medianos

34. Registros de Divulgación de Información Privada — Mantenimiento

Política: Toda divulgación de información privada a terceros se debe registrar y dichos registros se deben mantener por un período mínimo de cinco años.

Comentario: Esta política demuestra exactamente qué información ha sido divulgada a cuáles tercera personas, y que esas divulgaciones se han realizado en cumplimiento de la ley, la política de la organización y las prácticas comerciales generales. El mantenimiento de un diario de divulgaciones también es importante cuando se notifica a los receptores de información de los

errores encontrados en un expediente privado. Las agencias de crédito mantienen un registro de todas las terceras personas a quienes les han revelado detalles de las deudas y el historial de pagos de una persona. Si se detecta un error en un expediente, la agencia de crédito entonces está en condiciones de notificar inmediatamente a los receptores sobre la información corregida.

Políticas Relacionadas: “Divulgación de Información Privada a Terceros” y “Acceso a Divulgación de Registros de Datos Privados”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

35. Privacidad de la Información del Cliente

Política: La información que pueda ser vinculada directamente a un cliente en específico sólo se debe revelar a terceros cuando el cliente haya dado previo consentimiento por escrito, o si la Empresa X está legalmente obligada a divulgar la información.

Comentario: Esta política restringe la diseminación de información no autorizada de los clientes de un organización, y es pertinente para aquellas que suministran algún producto personal o servicio, tal como el seguro médico o terapia psicológica; como también puede ser pertinente para las aerolíneas, supermercados, y otras organizaciones que hacen seguimiento a los patrones de consumo de la clientela. La política puede interferir con el proceso de ciertas prácticas de acoplamiento de bases de datos a lo largo de diversas organizaciones, pero estas prácticas no tienen mucha aceptación con el público y son ampliamente consideradas una invasión de la privacidad. Algunas organizaciones van más allá de lo que es una política interna de esta naturaleza, e incluyen una versión distinta en el material que distribuyen a sus clientes. Varias compañías de seguros, por ejemplo, explícitamente informan a sus clientes acerca de sus políticas relacionadas con la divulgación a organizaciones de terceros. Hay quienes dicen que este tipo de comunicación con el cliente mejora la imagen pública de la organización y atrae nuevos clientes.

Políticas Relacionadas: “Información Estadística de los Registros de los Clientes”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

36. Compartir Información Privada

Política: La Empresa X no debe divulgar información específica de las cuentas de clientes, las transacciones, o las relaciones con terceros no afiliados para su uso independiente, a menos que la divulgación de la información sea para una agencia de información de reputación reconocida, cuando la información está relacionada con una solicitud del cliente para la ejecución de cierto acto, el cliente solicita la divulgación, la divulgación es requerida o permitida por ley, o el cliente ha sido informado acerca de la posibilidad de tal divulgación para propósitos de mercadeo o similares, y se le ha dado la oportunidad de declinar.

Comentario: Esta política tiene el propósito de conformar una política de privacidad para los clientes, lo que en algunas jurisdicciones puede ser obligatorio por ley. La política en cambio tiene la intención de brindar a la organización emisora básicamente un amplio espacio para proceder a libre albedrío. Por ejemplo, la organización emisora de la política se puede afiliar con otra organización, posiblemente en negocio asociado, y esto le permitiría el intercambio de información privada sin la previa notificación al cliente afectado. De igual manera, si la organización quisiera vender la información privada a terceros, sencillamente le daría aviso a sus clientes a tal efecto, y si cualquier cliente objetara, se eliminaría su información de la base de datos a ser compartida con terceros. Dado que esta política carece de sentido, no es recomendable.

Políticas Relacionadas: “Privacidad de la Información del Cliente” y “Divulgación de la Información del Cliente”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

37. Divulgación de Información Privada a Organizaciones Contratadas

Política: La Empresa X no debe vender, arrendar, o de alguna manera transferir información de clientes a terceras personas en ninguna forma, excepto cuando éstas firmen un acuerdo de confidencialidad a través del cual se les prohíba diseminar y hacer uso de la misma con fines no autorizados.

Comentario: Esta política garantiza a los clientes que sus datos privados se mantendrán confidenciales, a la vez que se brinda una flexibilidad a la organización para compartir datos privados con personas fuera de la organización, sin autorización del cliente. Por ejemplo, la política permite a la organización compartir

resúmenes de información del cliente con organizaciones ajenas dedicadas a la investigación de mercado, con consultores de minería de información y consultores de planificación estratégica. La política permite a la organización contratar con terceros cualesquiera de todas las funciones internas sin tener que notificar o conseguir el consentimiento del cliente. Una fusión o adquisición pudiera, en algunos casos, ser considerada como servicios contratados. Se recomienda el asesoramiento legal. La política permite la divulgación de información del cliente a las agencias del gobierno para fines de recaudación de impuestos, cumplimiento forzoso de la ley anti-discriminación y propósitos relacionados.

Políticas Relacionadas:“[Privacidad de la Información del Cliente](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

38. Divulgación de la Información del Cliente

Política: La Empresa X no debe divulgar a personas externas la información de sus clientes sin una autorización explícita emitida por escrito.

Comentario: Esta política le garantiza al cliente que puede hacer negocios con seguridad con la Empresa X. Una política semejante es útil para una organización cuando el simple hecho de que se sepa que cierto cliente hace negocios con ella, le resulte embarazoso. Esta política tiene la intención de ser publicada en un sitio de internet o en un panfleto, y no sólo para distribución interna para los trabajadores. Si la divulgación de información de los clientes se hace por mandato de ley, ésta información será revelada. Para unos, esto es obvio y por lo tanto no requiere su reiteración en la política en sí. Esta política también evita problemas de marcas registradas cuando un cliente declara que un negocio en particular está utilizando, de manera inapropiada, su nombre para atraer atención a su sitio en la web.

Políticas Relacionadas:“[Privacidad de la Información del Cliente](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

39. Divulgación de Datos Personales

Política: La información personal, incluyendo, sin limitantes, la agregada, resumida, anónima, los estudios de casos individuales, o información que identifica personas, que sea recopilada por la Empresa X no se debe vender, alquilar, transferir, entregar, o de alguna otra manera transferir a terceras personas.

Comentario: Esta política informa que la política de privacidad de la organización es absoluta y que no será comprometida. Esta política declara que la Empresa X no degradará la privacidad de sus clientes, sus trabajadores, u otras personas de quienes mantenga información personal. La política ilumina la manera en que la gerencia tiene un alto concepto de lo que ocurre en el área de la privacidad.

Políticas Relacionadas:“[Actividad de Monitoreo y Grabación](#)” y “[Aviso de Recopilación de Información](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

40. Divulgación de Receptor de Información del Cliente

Política: Cuando le sea solicitado por escrito, la Empresa X debe divulgar con prontitud, el nombre, dirección y número de teléfono de todas las terceras personas que reciben información privada acerca de cualquier cliente o persona.

Comentario: Esta política le permite al cliente o persona determinar quien ha recibido su información privada. La persona no tiene derecho de objetar esta divulgación inicial, sino determinar después del hecho, quién recibió la información. Esta política, en lugar de pretender un alto nivel de protección y control individual de la privacidad, obliga la responsabilidad de aquellos en cuyas manos está la información. La política también es útil en situaciones cuando se investiga un fraude de identidad, y si ha ocurrido, en la mayoría de los casos la persona ha de asumir la tarea de informar a todos los interesados de que alguien ha usado su nombre y crédito sin su autorización. Esta política supone que se mantienen registros de divulgación a terceros.

Políticas Relacionadas:“[Registros de Divulgación de Información Privada — Detalles](#)” y “[Acceso a la Información Personal](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

41. Notificación al Cliente de Solicitudes de Registros

Política: La Empresa X no debe liberar los registros de los clientes a terceros a menos que los clientes así lo soliciten, o a menos que se vea obligada a hacerlo por ley o reglamento, y sólo habiendo informado al cliente sobre dicha divulgación con dos semanas de anticipación.

Comentario: Esta política está dirigida a ajustar la política de privacidad que aplican varias organizaciones bajo la cual no divultan registros personales a terceros. La política impide que terceros utilicen la demanda como mecanismo de acceder a los registros personales que en otras instancias permanecerían confidenciales. Los clientes pueden utilizar la política en respaldo de su propia privacidad. El costo real para la organización es el relacionado con la actividad administrativa, y dirigido a las notificaciones enviadas en aquellas instancias donde se ha recibido una citación. Todos los costos legales asociados con el reto de una solicitud de registros son responsabilidad del cliente. El período de tres semanas es arbitrario, y podría ser ampliado hasta tanto la organización que mantiene los registros no sea suspendida por desacato a las autoridades por retardar la emisión de dichos registros.

Políticas Relacionadas: “Liberación de Información de la Organización” e “Información Personal de los Clientes”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

42. Aplicación de Política de Privacidad

Política: Toda la información de los clientes debe ser protegida de acuerdo con las políticas de privacidad vigentes para el momento en que se recopile la información, a menos que el cliente autorice otra iniciativa.

Comentario: Esta política informa al lector que la Empresa X considera que su política de privacidad es similar a un contrato legal. Esta perspectiva contractual se basa en el hecho de que los clientes suministran información bajo ciertas condiciones, y esperan que la organización receptora respete la política establecida. De acuerdo con esta política, la Empresa X no puede simplemente cambiar dicha política y utilizar la información del cliente recopilada bajo la política anterior y para objetivos no autorizados por dicha política anterior. Esta política implica mayores gastos generales sobre la empresa emisora, debido a que ahora

debe utilizar mecanismos para fechar la información timbrada de los clientes, y podría generar identificadores especiales que reflejen la política de privacidad que aplique a un registro de cliente. Se pueden requerir diferentes listas de correo y rutinas de procesamiento para manejar dos o más series de clientes, de alguna manera consistentes con diferentes políticas de privacidad. Esta política refleja una tendencia en el área de políticas de privacidad publicadas en Internet. Los entes reguladores gubernamentales cada vez están comprometiendo más a las empresas para que mantengan lo prometido en sus políticas de privacidad, actuando como si éstas fueran contratos legales.

Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición” y “Autorización para Inclusión en Sistemas de Datos Privados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

43. Privacidad de Información de Contacto de Remitentes

Política: No se deben revelar a terceros las direcciones de correos electrónicos y los números telefónicos de las personas que intercambian información con todos los usuarios de los sistemas informáticos de la Empresa X, a menos que se obligue legalmente a la Empresa X.

Comentario: Aunque el público piensa que las direcciones de los correos electrónicos y los números telefónicos de las personas con las que intercambian información son confidenciales, algunas veces, esta información se puede compartir con una empresa telefónica u otro proveedor de sistemas informáticos sin la autorización de los usuarios correspondientes. La política garantiza a los usuarios la confidencialidad de con quien intercambian información. La política asume que la organización ya dispone de una política de privacidad en cuanto al contenido de estas comunicaciones. La política es un intento de impedir que la información de los sistemas informáticos sea utilizada por terceros. Esta política está dirigida a los proveedores de servicios de sistemas informáticos, tal como un proveedor de servicios de Internet o una empresa telefónica.

Políticas Relacionadas: “Información Personal de los Clientes” y “Registros de Divulgación de Información Privada — Mantenimiento”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

44. Anonimato del Cliente

Política: La Empresa X debe suministrar mecanismos para que los clientes escojan si prefieren mantener su anonimato al utilizar los sistemas de la Empresa X.

Comentario: La intención de esta política es darle al cliente una idea clara de lo que significa identificadores de usuarios anónimos, remitentes anónimos, dinero electrónico anónimo, y mecanismos anónimos similares. Esta política está diseñada originalmente para aquellas organizaciones que ofrezcan servicios públicos de computación y de comunicaciones, aunque las mismas ideas aplican para los grupos de discusión en intranet y a los buzones de sugerencias internos automatizados.

Políticas Relacionadas: “Identificadores de Usuarios Anónimos” y “Privacidad de la Información del Cliente”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

45. Identificación de Clientes Famosos

Política: Los trabajadores no deben dar a conocer públicamente la identidad de los clientes famosos cuando éstos estén presentes, no deben hablar sobre estos clientes sino con otros trabajadores de la Empresa X, y no deben revelar la identidad de los mismos a menos que estén realizando una actividad comercial.

Comentario: Esta política mantiene la privacidad de los clientes famosos, y los hace sentir a gusto en su relación comercial con la Empresa X. La política prohíbe el chismorreo y las conversaciones innecesarias que puedan llevar a calumnias o a acusaciones por difamación. Esta política también es consistente con la seguridad que da el mantener un bajo perfil.

Políticas Relacionadas: “Actividad de Monitoreo y Grabación” e “Identificadores de Usuarios Anónimos”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

46. Información Estadística de los Registros de los Clientes

Política: La información estadística que proviene de los registros de los clientes, no se debe revelar a terceros fuera de la Empresa X, a menos que no se pueda identificar al cliente a través de dicha información.

Comentario: Esta política impide que los trabajadores distribuyan informes a terceros, los cuales puedan revelar de manera accidental la identidad de un cliente o la información relacionada con este. Esta política es importante en la preparación de los informes anuales, los formularios gubernamentales, y para todos los mecanismos de informes. La palabra "estadística" se podía reemplazar por "numérica". La idea detrás de esta política es que se debe resumir o agrupar la información de los clientes de tal manera que, al ser divulgada no dañe la privacidad de los clientes. Si no se puede cambiar la información agrupada para ocultar la identidad de los clientes, entonces no se debe revelar dicha información. Puede que la organización quiera cambiar la política para que incluya que un nivel gerencial autorice la revelación de la información estadística, ya que la decisión de no revelar la identidad de los clientes se puede convertir en una tarea compleja y lenta.

Políticas Relacionadas: “Privacidad de la Información del Cliente” y “Restricciones a la Recopilación de la Información”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

47. Divulgación del Registro de las Actividades del Cliente

Política: Los registros que reflejen las actividades de los usuarios de los computadores o de los que se benefician de estos, no se deben revelar a terceros, a menos que la Empresa X se vea obligada por una orden remitida por un tribunal, por una ley o por una regulación, o mediante una autorización por escrito de los individuos correspondientes.

Comentario: Esta política protege la privacidad de aquellos individuos cuyas actividades aparecen en los registros. La política cubre las investigaciones bibliográficas suministradas por las bibliotecas, las historias de las cintas alquiladas de video, los registros de transacciones bancarias, los registros de comprador frecuente en los supermercados, y demás información recopilada. Están cubiertos además, los registros de las actividades de los usuarios habituales de los computadores. Algunas organizaciones querrán restringir el alcance de esta política haciendo referencia a registros específicos.

Políticas Relacionadas: “Restricción de Privilegios — Necesidad de Conocer” e “Información de Registro del Cliente”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

48. Cumplimiento de la Privacidad

Política: Los trabajadores no deben permitir una violación de la privacidad de la Empresa X o dejar de observar el derecho a la privacidad de la Empresa X, a menos que se obtenga una autorización de la alta gerencia.

Comentario: Esta política define parcialmente el derecho a la privacidad que tiene una organización. La intención es informar a los empleados sobre la existencia de dicho derecho, que no deben obviarlo a menos que la alta gerencia lo autorice, y que deben defenderlo. Una política como ésta debe ser importante cuando se tiene que proteger la información confidencial de un adversario en un juicio. La idea de privacidad para una organización en contraste con un individuo, es diferente y puede resultar extraña para algunas personas. Para compensar esta falta de conocimiento, puede que algunas organizaciones quieran ampliar estos conocimientos con los derechos de privacidad de la Empresa X. Por ejemplo, los empleados no deben llevar a cabo contratos en los que acuerdan revelar información confidencial de la Empresa X, a menos que reciban una autorización de la gerencia. De igual manera, se puede evitar una solicitud para una orden de registro si las partes acuerdan una revisión policial. Los empleados no deben suministrar tal acuerdo sin la autorización de la alta gerencia. Para una política como ésta, se recomienda consultar a los asesores legales internos.

Políticas Relacionadas:“[Acuerdos de Confidencialidad de Terceros](#)” y “[Divulgación de Información a las Autoridades](#)”

Política Dirigida a:Usuarios finales y gerencia

Ambientes de Seguridad:Todos

49. Consentimiento para Acciones Cuestionables en los Sistemas

Política: Cuando exista inseguridad en el desempeño de una actividad con un computador, los trabajadores de la Empresa X deben informar a los afectados sobre las acciones que piensan llevar a cabo, el propósito de dichas acciones, y los impactos potenciales que estas pueden ocasionar en los receptores de la información, y deben contar con autorización de los afectados o el permiso de un vicepresidente.

Comentario: Esta política está dirigida a impedir que los trabajadores realicen actividades con los computadores que puedan afectar a terceros. Por ejemplo, el lanzamiento de un producto nuevo, puede haberle facilitado a algunas organizaciones, la publicidad directa por correo, con unos costos muy inferiores y con información personal de varios individuos. Preocupados por la violación de privacidad, más de 30.000 personas objetaron el estar incluidos en la base de datos y el proyecto fue abandonado. Para algunas organizaciones, la política puede resultar muy imprecisa de la manera aquí expuesta, y puede que necesite ejemplos específicos, tales como los que manejan las violaciones de privacidad.

Políticas Relacionadas:“[Responsabilidad en la Seguridad Informática](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

50. Autorización de Acceso a los Registros Individuales

Política: Los pacientes no pueden ver sus registros médicos personales sin la autorización previa del proveedor de atención médica que generó dichos registros.

Comentario: Esta política reconoce que la privacidad y los derechos profesionales de cortesía que los proveedores de asistencia médica son más importantes que los derechos de los pacientes de conocer su condición médica. Muchas jurisdicciones poseen leyes que regulan específicamente sobre el acceso de un paciente a informarse sobre su salud. Puede existir un conflicto entre los objetivos del paciente y el proveedor de asistencia sanitaria. Por ejemplo, un paciente puede querer saber sobre el estado de su salud, pero el doctor no quiere revelar esta información, pensando que esto puede empeorar la situación. Un doctor también puede restringir el acceso a los registros del paciente por temor a que estos registros se pueden utilizar en juicios de mala práctica. Algunas leyes garantizan el derecho de acceso a los registros sobre el estado de salud de uno mismo, pero este derecho no aplica a todos los tipos de pacientes. El título de la política, intencionalmente, es genérico y abarca más allá de la industria de asistencia sanitaria, para demostrar que la idea de los derechos creados sobre los registros se puede aplicar en otras áreas aparte del área de atención sanitaria.

Políticas Relacionadas:“[Acceso al Archivo del Personal](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

51. Divulgación de Usos Propuestos de Información Personal

Política: Antes de que un cliente coloque una orden o revele alguna información personal, todos los representantes de la Empresa X deben informar a los clientes la forma en que dicha información se va a utilizar.

Comentario: Esta política garantiza que toda la información personal se ha recopilado de manera justa y transparente para los consumidores. La política elimina toda ambigüedad acerca de la naturaleza de la relación que se va a establecer entre un consumidor y una organización. La mayoría de los consumidores no pondrán reparos, pero los que los tengan, se colocarán en una categoría especial. Debido a que las discusiones sobre una política como ésta, podría poner en peligro una venta, muchas organizaciones solventarán estas situaciones una vez concluida la venta, otras optarán por un rol más pasivo, al incluir una notificación acerca del uso de información personal en publicidades o folletos. Aquellas organizaciones que como principio, no revenden direcciones de correo electrónico u otra información personal, piensan que esta política les proporciona una ventaja competitiva.

Políticas Relacionadas: “[Opción de Participación en Sistema de Datos Privados](#)”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

52. Acceso al Archivo del Personal

Política: Se debe permitir a los empleados tanto examinar como elaborar una copia de la información que aparece en su archivo personal.

Comentario: El sólo permitirles a los empleados que pueden revisar sus archivos personales, los limita en forma rigurosa a rectificar errores. Esta política les permite a los empleados recopilar la información que necesitan, llevarla a casa, a un abogado o a algún tercero. El permitir a los empleados hacer una copia, les permite elaborar mejores cartas y solicitudes para cambiar sus archivos. Esta política provee un mecanismo para mejorar la integridad de la información y es consistente con la ética de que los empleados deben

tener control de la información que existe acerca de ellos. Un efecto secundario positivo de esta política es que la misma disuade la adición de información incorrecta en los archivos personales. Al mismo tiempo la existencia de la política puede promover la existencia de archivos secretos no autorizados que los trabajadores no deben revisar. La política podría ser ampliada para que aplique a todos los trabajadores, inclusive contratistas, consultores y trabajadores temporales.

Políticas Relacionadas: “[Acceso a la Información Personal](#),” “[Sistemas Secretos](#),” y “[Distribución de los Registros del Personal](#)”

Política Dirigida a: Usuarios finales y gerencia

Ambientes de Seguridad: Todos

53. Revisión del Archivo del Empleado

Política: Todos los empleados que deseen revisar su archivo personal, deben someter una petición por escrito a la gerencia de Recursos Humanos, y revisar sus archivos en el momento asignado, durante horas laborables, y en la presencia de un representante de Recursos Humanos.

Comentario: Esta política está dirigida a impedir que la gerencia mantenga información inapropiada en archivos personales. Esta política requiere que se introduzca una solicitud formal, lo cual da a la gerencia la oportunidad de eliminar referencias fuera de lo normal o material inapropiado. La eliminación de este material ayuda a prevenir discriminación o juicios por acoso. La política genera un ambiente controlado en el cual las preguntas acerca del registro se pueden manejar inmediatamente a través de la gerencia de Recursos Humanos. Esta solución inmediata de problemas, puede prevenir agravios, chismorreo innecesario y juicios sin garantías. La presencia de este representante significa también que se puede prevenir el copiado o la remoción de material de ese archivo. También se pueden establecer límites sobre el número de veces en que puede ser revisado un registro, aunque algunas veces estos límites no sean necesarios.

Políticas Relacionadas: “[Distribución de los Registros del Personal](#)” y “[Autorización de Acceso a los Registros Individuales](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

54. Declaración Explicativa del Empleado

Política: Si los empleados objetan la exactitud, la importancia o la integridad de la información que aparece en sus archivos personales, se les debe dar una oportunidad para incorporar una declaración adicional.

Comentario: Esta política permite a los empleados contar su versión sobre una tema en particular descrito en sus archivos personales. Si la organización decide no solicitar ajustes a un archivo personal, respondiendo a las quejas de un empleado, entonces se puede insertar una declaración. Puede que el empleado no presente una queja formal acerca de la información en el archivo, pero puede optar por insertar una explicación, debido a que el registro tiende a ser confuso sin la información adicional. El añadir una declaración suplementaria puede ser un privilegio único, o se puede utilizar repetidas veces para cada información que haya obtenido respuesta. La política también se puede utilizar en personas que no son empleados. No existe, bajo esta política y en forma deliberada, el requisito de que se elimine o corrija la información incorrecta.

Políticas Relacionadas: “[Acceso a la Información Personal](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

55. Información Personal Incorrecta

Política: Cada vez que se notifique a la Empresa X sobre la existencia de información personal errada en sus registros, esta debe corregir inmediatamente dicha información o anexarle un indicativo de que la misma está en discusión y que se alega su inexactitud.

Comentario: Esta política garantiza que los registros que contengan información personal son vigentes y correctos. Si los errores de los registros personales no son corregidos inmediatamente, los individuos cuya descripción se encuentra en esos registros van a sufrir grandes daños. Por ejemplo, si una agencia que proporciona información sobre la solvencia de empresas y particulares no corrigió, o calificó de incorrecta, información errada sobre una bancarrota, la persona descrita en el registro sufrirá daños personales. Esta política no requiere una modificación de un registro si el personal de la Empresa X no está seguro de la información corregida. Aquí es aconsejable una etiqueta que especifique la existencia de una disputa. Dentro de esta política se asume que una política asociada le ha

otorgado a las personas descritas en los registros personales el derecho o la oportunidad de revisar la información de los registros de la Empresa X. Mientras que esta política refleja la existencia de una buena práctica en el área de administración de la base de datos, resulta útil dejar constancia escrita que las personas cuya descripción aparece en los registros, tengan la garantía que dicha información será tratada respetuosa y cuidadosamente.

Políticas Relacionadas: “[Acceso a la Información Personal](#)” y “[Divulgación de Receptor de Información del Cliente](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

56. Integridad del Registro Personal

Política: La gerencia debe realizar esfuerzos adicionales para garantizar que la información personal que permanece en la Empresa X es correcta, oportuna, relevante e íntegra.

Comentario: Esta política requiere que la gerencia mantenga registros contentivos de información personal. Con esta política, se requiere que la gerencia haga correcciones si la organización ha sido notificada sobre errores en un registro por la persona descrita en el mismo. Esto resulta importante para aquellas organizaciones que utilizan normalmente información personal como parte de sus negocios habituales, en oposición a aquellas organizaciones que utilizan información personal en actividades internas de administración de Recursos Humanos. Esta es una buena política general con la cual pueden contar otras políticas, y también resulta apropiada para resumir una política. Puede que algunas organizaciones quieran añadir una descripción de "información personal" o simplemente suministrar ejemplos. La información personal incluye información sobre el personal, pero se puede definir como una categoría más amplia. La información personal de los clientes podría estar dentro del alcance de esta política, pero técnicamente no se considera información sobre el personal. En esta política, se puede utilizar la palabra "privada" en vez de "personal".

Políticas Relacionadas: “[Investigación de Errores](#)” e “[Información de Contacto del Empleado](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

57. Manejo del Registro Personal

Política: Se deben establecer procedimientos documentados para manejar la información personal, se debe hacer un seguimiento estricto y actualizar dicha información regularmente.

Comentario: Esta política requiere que los grupos operacionales que manejan datos privados conceptualicen claramente, documenten, y sigan fielmente los procedimientos establecidos. La existencia de estos procedimientos va a garantizar un manejo seguro y consistente de los datos privados, así como lo ofrecen a los auditores internos un punto de referencia en sus evaluaciones. De existir un problema que haya sido revelado al público, o un juicio, estos procedimientos se pueden utilizar igualmente para evidenciar que la gerencia tomó los pasos necesarios para proteger la información privada. Estos procedimientos van a manejar regularmente la recepción rutinaria y no rutinaria de información privada, la manipulación, el procesamiento, el almacenamiento y la retención de estos datos, su diseminación y transmisión así como la eliminación y la destrucción de los mismos

Políticas Relacionadas: “Revisión de Registros de Operadores de Computadores” y “Procedimientos de Respuesta a Intrusión”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

58. Uso del Registro Personal

Política: La gerencia debe realizar esfuerzos adicionales para garantizar que la información personal se va a utilizar sólo para lo que se diseñó originalmente y que las precauciones para evitar su mal uso son efectivas y apropiadas.

Comentario: Esta política requiere que la gerencia garantice que la Empresa X no utiliza la información sino para lo que fue diseñada originalmente. La política también puede garantizar que la información no se va a transferir a terceros sin que la persona que la haya suministrado originalmente tenga conocimiento de esto o lo haya autorizado. Esta es una buena política general y con la que pueden contar otras políticas, así como resulta apropiado como resumen de una política. La información personal también incluye información

sobre el personal, pero puede ser una categoría definida más ampliamente. La información personal de los clientes estaría dentro del alcance de esta política, aunque no sea información sobre el personal. En esta política la palabra "privada" puede ser utilizada en vez de "personal".

Políticas Relacionadas: “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

59. Registro del Acceso a la Información Privada

Política: Deben establecerse controles de acceso para todo sistema de producción que contenga información catalogada como "privada", de forma tal que todo acceso a dicha información iniciado por un usuario sea registrado, identificando al individuo cuya información fue accedida, al usuario que está haciendo la petición de acceso, la fecha y la hora.

Comentario: Esta política garantiza que existe la suficiente inspección, de forma que posteriormente se pueda determinar quién accedió a cuál información privada y cuándo. Esta política está a favor de la privacidad y por lo general requiere el desarrollo de software adecuado. Esto se debe a que pocos de los sistemas de manejo de bases de datos o los paquetes de control de acceso están provistos de esta especificidad en sus sistemas de registro. Esta política permite una rigurosa aproximación a la protección de la privacidad. Esta política asume que se ha adoptado un sistema de clasificación de los datos y que la palabra "privado" tiene un significado bien entendido dentro de la organización. Las palabras "iniciado por un usuario" son importantes porque eximen al software de poder acceder a información privada dentro del proceso de mantenimiento del sistema automatizado.

Políticas Relacionadas: “Registros en Sistemas y Aplicaciones Sensibles,” “Arquitectura de Sistemas para Registro de Actividades,” y “Originador de Transacciones”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

60. Uso de la Información Personal para Nuevos Propósitos

Política: La información personal acerca de empleados, consultores o contratistas que ha sido recopilada para un propósito, no debe ser utilizada para otro fin sin el claro y manifiesto consentimiento de las partes a las que esta información incumbe.

Comentario: La intención de esta política es evitar el mal uso de la información personal con fines distintos de los originales. Si un ciudadano de un gobierno reveló determinada información acerca de su declaración de impuesto, de forma tal que el gobierno pudiera aplicar las leyes impositivas, esta política prohibiría que la información sobre esta declaración sea utilizada para cualquier otro propósito. Esta política reduce la flexibilidad que tendría la gerencia de emplear la información en la manera que deseé. La existencia de esta política podría animar a las personas para que revelen información que de otra manera no desplegarían. Se trata de una política de privacidad ampliamente suscrita, sin embargo, en lugar de que el público en general apoye esta idea, muchas compañías y agencias gubernamentales la consideran demasiado restrictiva. En esta política la palabra "confidencial" podría ser utilizada en lugar de "personal".

Políticas Relacionadas: "[Uso Personal del Teléfono](#)" y "[Uso Distinto al Empresarial de la Información de la Organización](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

61. Enlace de Información Anónima

Política: Los sistemas informáticos y el personal de la Empresa X no deben enlazar información anónima con información que permita la identificación personal, a menos que las personas involucradas hayan dado su consentimiento.

Comentario: Esta política encara un serio problema asociado principalmente con las actividades de negocio de Internet. Determinada información personal que es anónima a menudo es recopilada sin el conocimiento de los usuarios involucrados. Posteriormente, esta información puede ser enlazada con información que permita la identificación personal, como por ejemplo los patrones de compra del consumidor, de manera que se pueda formar una descripción más reveladora acerca de su comportamiento individual o sus actividades. Esta

política prohíbe este enlace en un esfuerzo por proteger la privacidad de las personas involucradas. Al adoptar esta política, una organización puede asegurarles a los usuarios que realmente se preocupa por su privacidad. Esta política es adecuada para ser desplegada en una página web. Las palabras en esta política son estrictas. Una versión menos restrictiva podría reemplazar las palabras referidas a pedir el consentimiento por palabras acerca de una fuerte advertencia.

Políticas Relacionadas: "[Uso de la Información Personal para Nuevos Propósitos](#)," "[Enlaces con Información Privada](#)," y "[Uso del Registro Personal](#)"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

62. Información Personal de los Clientes

Política: Todos los registros de los clientes que contengan información personal que se encuentren en poder de la Empresa X deben utilizarse únicamente con fines directamente relacionados con el negocio de la Empresa X y únicamente pueden ser revelados a terceros con el consentimiento del cliente o si la Empresa X ha recibido una citación u orden judicial.

Comentario: Esta política prohíbe la utilización de la información personal o confidencial acerca de los clientes con fines distintos de los originales. Esta política prohíbe igualmente la venta, alquiler, intercambio o cualquier otro método para transmitir la información personal a otras organizaciones que podrían utilizarla para solicitar negocios de los clientes de la Empresa X. El término "en posesión de la Empresa X" se utiliza porque la Empresa X tendrá problemas para mantener el control sobre los registros de los clientes que no se encuentren en su posesión, a pesar de que esto podría ser factible en caso de que la posesión la tengan empresas subcontratadas. Esta política podría identificar específicamente las clases de información que no pueden ser desplegadas externamente. Esta política podría ser modificada para incorporar una excepción cuando quien recibe la información es una agencia gubernamental.

Políticas Relacionadas: "[Uso de la Información de Contacto del Cliente](#)"

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

63. Acceso del Cliente a Información Personal

Política: A los clientes se les debe dar la oportunidad de obtener una confirmación de la Empresa X de que la información personal acerca de ellos se encuentra almacenada en los sistemas de la Empresa X y una explicación acerca de la naturaleza de esta información.

Comentario: Esta política informa a los clientes y a los empleados que los clientes pueden legítimamente recibir ciertas clases de información interna de la Empresa X. Esta política no libera la información por sí misma, sino que únicamente libera la "metadata", es decir, la información acerca del cliente. Por lo general habrá menos discusiones acerca de la "metadata" que acerca de información específica. Los reglamentos de algunas industrias, como por ejemplo la industria de informe de crédito de los clientes, requerirán que se divulgue información personal específica y no únicamente la "metadata". Esta política favorece al cliente; sin embargo, requiere muy poco esfuerzo para que la empresa la adopte.

Políticas Relacionadas: ["Recopilación de Información de Clientes"](#) e ["Información Personal para el Funcionamiento del Negocio"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

64. Uso de la Información de Contacto del Cliente

Política: La información de contacto recopilada acerca de los clientes o clientes potenciales debe utilizarse únicamente para propósitos internos de la Empresa X.

Comentario: Esta política garantiza que la información de contacto del cliente no se utilizará con otro fin que el necesario para que la empresa pueda proveer un producto o servicio. Este tipo de política es particularmente apropiado para aquellas organizaciones que proveen un producto o servicio acerca del cual el cliente podría sentirse incómodo o muy consciente. La existencia de una política como ésta podría además generar negocios adicionales para estas organizaciones debido a que algunas personas pudieran haberse abstenido de convertirse en clientes a menos que su nombre e información de contacto se encuentren en una lista. La preocupación más predominante se refiere a la venta o intercambio de información acerca del teléfono y dirección del cliente, lo cual puede conducir a

mensajes de correo no deseados o solicitudes telefónicas. Esta política está dirigida para ser distribuida a los clientes y clientes potenciales.

Políticas Relacionadas: ["Información Personal de los Clientes"](#) y ["Divulgación de Información Privada a Organizaciones Contratadas"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

65. Información Personal Incluida

Política: Los sistemas informáticos de la Empresa X no deben emplear números seriales secretos, números de identificación del personal secretos ni cualquier otra clase de mecanismo secreto que pudiera revelar la identidad o las actividades de los clientes.

Comentario: Esta política responde al uso reciente que se le da a los números secretos de identificación en algunas aplicaciones comerciales para computadores personales. Utilizando estos números, es posible rastrear un archivo hasta su creador. Si los usuarios no fueron informados acerca de estos números, pudieron haber comprometido su privacidad sin saberlo en el momento en que colocaron archivos en Internet o en otro foro público. Esta política obtiene nuevos negocios para los sistemas de comercio electrónico al asegurarle a los clientes que no serán engañados al llevar a cabo una transacción, para posteriormente descubrir que existían mecanismos secretos utilizados para comprometer su privacidad. Esta política impulsa la causa de la privacidad, pero a expensas de investigaciones criminales. Esta política está destinada a ser desplegada en una página web, en un boletín electrónico o en cualquier otro medio público. Para los ambientes de comercio en Internet, puede hacerse especial mención a las "cookies" que son el mecanismo que de forma arbitraria identifica a los clientes.

Políticas Relacionadas: ["Enlaces Entre la Información Privada y la Identificadora"](#) y ["Cookies para Inicios Automáticos de Sesión"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

66. Identificadores Personales en Ubicaciones Públicas

Política: Con excepción de las claves de cifrado y de los certificados digitales, ningún identificador personal debe aparecer en una ubicación accesible públicamente,

manejada o controlada por la Empresa X, incluyendo páginas web, sitios de comercio en Internet, manuales de productos o publicidad en revistas.

Comentario: Esta política preserva la privacidad tanto de los clientes como de los empleados. Si los identificadores personales no están disponibles, entonces las actividades de estas personas no pueden ser rastreadas hasta ellas mismas. Esta política también evita el robo de identidad. Si los identificadores personales, números telefónicos, números de tarjetas de crédito, direcciones de correo electrónico y demás identificadores no aparecen en ubicaciones accesibles públicamente, no pueden ser ni robados ni utilizados. Esta política no evita que la organización pueda colocar identificadores personales en ubicaciones restringidas, como por ejemplo la lista de pedidos por Internet para ser enviados próximamente. Un cliente únicamente podría ver su orden mediante un identificador de usuario. En algunos casos la palabra "real" podría ser añadida al principio de esta política para distinguir entre identificadores personales reales y ficticios.

Políticas Relacionadas: "[Información Personal Incluida](#)" e "[Identidad en Internet](#)"

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

67. Inteligencia de Números de Cuentas

Política: La Empresa X no puede utilizar identificadores externos significativos como sus propios números internos de cuenta de los clientes.

Comentario: Esta política evita el robo de identidad. Por conveniencia, muchas organizaciones utilizan identificadores personales en sus estados de cuenta mensuales. El uso de identificadores personales invita al abuso de terceros que pueden obtener este número cuando revisan los desechos o cuando reciben copias de los estados de cuenta de los clientes. Estos identificadores deben ser salvaguardados como información confidencial. Esta política demostrará que la Empresa X está realmente tratando de prevenir el aumento ya tan común del abuso conocido como fraude de identidad.

Políticas Relacionadas: "[Códigos de Identificación para Soporte Técnico](#)" y "[Acceso a la Información Personal](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

68. Enlaces Entre la Información Privada y la Identificadora

Política: Debe mantenerse el enlace entre la información de identificación personal y los datos privados únicamente hasta llevar a cabo el propósito para el cual se recopilaron originalmente los datos.

Comentario: Esta política evita que los archivos de registros médicos, las bases de datos de actividades de los clientes o cualquier otra información que contenga identificadores personales violen inadvertidamente la privacidad de las personas. Utilizada en la mayoría de los casos para la investigación, esta política permite que la información de fondo sea recopilada y analizada para posteriormente borrar todos los enlaces a identificadores personales. Esto puede tomar la forma de un archivo de comunicación personal y un archivo de investigación de datos para cada individuo. Los números seriales o apuntadores hacen la referencia cruzada para conectar los archivos. Una vez que la recopilación de la información ha terminado, la información de la referencia cruzada se elimina. En este momento, toda la información está disponible pero la privacidad del individuo está garantizada. Más allá de la investigación, esta política puede ser también adecuada para determinadas actividades comerciales. Por ejemplo, una cadena de librerías que disponga de un programa de comprador frecuente podría crear un archivo de contactos que podría ser utilizado para solicitudes y servicio al cliente y mientras tanto mantener un archivo de investigación de mercado que contenga todas las compras realizadas sin la información de contacto.

Políticas Relacionadas: "[Enlaces con Información Privada](#)," "[Identificadores de Usuarios Anónimos](#)," e "[Informes de Incidentes](#)"

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

69. Enlaces con Información Privada

Política: Los sistemas informáticos no deben soportar ningún enlace entre información privada y otros tipos de información relacionada con la misma persona sin la aprobación de la Gerencia de Seguridad Informática.

Comentario: Para garantizar la privacidad de los individuos, esta política limita el número de personas que tienen acceso a información personal. En la industria del cuidado personal, esta política prohíbe el establecimiento de enlaces entre la información de cuidado personal y otros tipos de información como datos financieros o datos de los empleados. Esto

impediría, por ejemplo, que el personal del departamento de facturación de un hospital pueda conocer el tratamiento específico que se le administra a un paciente. Existe un potencial efecto secundario adverso en esta política. Podría disuadir el establecimiento de un archivo de información del cliente (CIF, por sus siglas en inglés) que describe todas las distintas relaciones que mantiene con un individuo en particular. Los CIFs y las bases de datos parecidas son comunes en la industria bancaria y también son utilizadas en otras partes para permitir que el personal de servicio al cliente pueda responder a un individuo de una manera inteligente con información actual. La aprobación requerida permitirá que una organización tenga tanto un CIF como una base de datos similar e igualmente una política de privacidad como ésta. La palabra "enlace" es deliberadamente vaga de forma tal que se aplica tanto a un diccionario de datos corporativos, a la red interna o las bases de datos para obtener correspondencias.

Políticas Relacionadas:“Enlaces Entre la Información Privada y la Identificadora” y “Enlace de Información Anónima”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

70. Opción de Participación en Sistema de Datos Privados

Política: Antes de proceder a la implantación de un nuevo o sustancialmente modificado sistema informático que maneje datos privados, las personas involucradas deben tener la oportunidad de escoger si desean participar en el nuevo sistema.

Comentario:Esta política le da a las personas descritas por el sistema de datos privados la oportunidad de no participar de un nuevo sistema. Esto requerirá que el proveedor del sistema sea proactivo, contacte a los individuos y les explique el nuevo sistema. Un ejemplo involucra la correspondencia de bases de datos, el enlace de dos bases de datos previamente conectadas para obtener una nueva información. Esta es la razón por la que esta política requiere la obtención del permiso antes de la implantación. Después de la implantación la privacidad de los individuos involucrados puede ser violada. Algunos podrían decir que los individuos deberían ser excluidos por descarte y que se les dé el derecho de participar. Esta política, que permite a los individuos no participar está más de acuerdo con el mantenimiento de prácticas normales pro-negocio.

Políticas Relacionadas:“Autorización para Inclusión en Sistemas de Datos Privados,” “Clientes Rechazan Correo Directo No Solicitado,” y “Divulgación de Usos Propuestos de Información Personal”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

71. Recordatorio de Política de Privacidad

Política: A todos los clientes de la Empresa X se les debe enviar anualmente una copia de la política oficial de privacidad de la Empresa X y las instrucciones informándoles cómo pueden dejar de participar de las actividades de compartimiento de datos de la Empresa X.

Comentario:Esta política especifica una frecuencia mínima para la remisión a todos los clientes de la política de privacidad revisada. Igualmente asegura que los clientes reciban recordatorios regulares acerca de las formas en las que pueden restringir el uso de información acerca de ellos. Las palabras "actividades de compartimiento de datos" en la política se refieren a las maneras en las que la Empresa X comparte la información del cliente con otras organizaciones. Si los clientes le dicen a la Empresa X que no desean formar parte de estas actividades de compartimiento de datos, pueden declinar la participación. El método utilizado para la transmisión de la copia de la política de privacidad no se determina deliberadamente porque podría ser un inserto dentro de un sobre que contenga una factura, un mensaje impreso dentro de una declaración, un mensaje electrónico o cualquier otro método de comunicación.

Políticas Relacionadas:“Clientes Rechazan Correo Directo No Solicitado” y “Aviso de Cambio en Política de Privacidad”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

72. Autorización para Inclusión en Sistemas de Datos Privados

Política: Para que los individuos interesados puedan ser incluidos dentro de cualquier sistema de la Empresa X que maneje datos privados, deben específicamente elegir participar en el sistema.

Comentario:Esta política evita que la gerencia introduzca sistemas en donde se almacenan datos privados en contra de los deseos de los individuos

descritos dentro del sistema. Esta aproximación elimina muchas cuestiones relacionadas con la privacidad, pero puede también eliminar algunas oportunidades de negocio. Algunas organizaciones desearían instaurar una política como ésta solamente para cierto tipo de datos en lugar de aplicarla para toda la información privada. No se hace mención a la implantación del sistema debido a que los individuos no se describirían en este tipo de sistema si no hubieran específicamente elegido estar en él. El sistema no podría ser implementado inicialmente si no existieran datos almacenados en él. Esta política está a favor del cliente en lugar de estar a favor del negocio. Sería una ventaja de negocio adoptar esta política si el sistema contemplado o la actividad de negocios involucra asuntos extremadamente privados.

Políticas Relacionadas:“[Opción de Participación en Sistema de Datos Privados](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

73. Control del Individuo sobre el Uso de sus Datos Personales

Política: Si un individuo o cliente decide revocar el permiso que dio para que la Empresa X utilice sus datos personales, la Empresa X debe actualizar rápidamente sus registros y asegurarle que sus deseos se han cumplido.

Comentario:Esta política asegura a los clientes que pueden cambiar de parecer en cualquier momento acerca de la autorización que le dieron a la Empresa X de utilizar o compartir sus datos personales. Muchas organizaciones consideran al proceso de autorizaciones como si se tratara de un evento anual que permite cambiar el estatus del individuo si éste lo desea; otras, consideran al proceso como un evento que ocurre únicamente cuando se establece la relación con el individuo. Esta política reconoce que se trata de una ventana que se encuentra permanentemente abierta y que permite que el individuo cambie de parecer en cualquier momento. Si se ha autorizado compartir los datos personales con terceros, esto no puede ser revertido en realidad. Sería aconsejable añadir a esta política una declaración en la que se les asegure a los clientes que no habrá cargo o costo asociado a este

cambio en su estatus. Es también recomendable dar instrucciones claras acerca de cómo someter este tipo de notificación al personal de la Empresa X.

Políticas Relacionadas:“[Aplicación de Política de Privacidad](#)” y “[Opción de Participación en Sistema de Datos Privados](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Todos

74. Uso de Información Específica Respecto de la Ubicación

Política: La Empresa X no utilizará información relativa a la ubicación precisa de sus clientes o empleados con dispositivos inalámbricos o permitirá que otras organizaciones comerciales utilicen esta información con propósitos de mercadeo a menos que exista una autorización específica de cada individuo.

Comentario:Esta política controla el uso de información obtenida de sistemas de ubicación específica. Estas nuevas funciones representan oportunidades para el mercadeo improvisado. De la manera como está escrita, esta política es bastante benigna y permisiva. En la mayoría de los casos, los usuarios querrán crear su perfil, indicando en qué se interesan, por lo que sería necesario indicar que sí desean participar. Si se utilizan estas nuevas funciones de ubicación específica sin obtener previamente la autorización del usuario, podría presentarse un problema de relaciones públicas. Esta política deliberadamente deja de mencionar el hecho de compartir estos datos con agencias gubernamentales debido a que las leyes y normas acerca de esto todavía no se han determinado. Esta política proyecta una imagen positiva de la organización pero a la vez implica muy poco esfuerzo para que la misma la adopte de manera de mantenerse en cumplimiento. Esta política sería adoptada en la mayoría de los casos por un proveedor de servicios como por ejemplo un proveedor de Internet o de aplicaciones, pero podría ser adoptada por otros tipos de organizaciones que soporten las comunicaciones inalámbricas.

Políticas Relacionadas:“[Información Personal de los Clientes](#)” y “[Uso de Pequeños Computadores Portátiles](#)”

Política Dirigida a:Usuarios finales

Ambientes de Seguridad:Medianos y altos

75. Remoción de Individuos de la Base de Datos

Política: Si un individuo solicita ser removido de la base de datos de clientes o prospectos de la Empresa X, los empleados deben eliminarlo inmediatamente de la base de datos.

Comentario: Esta política asegura que los empleados de la Empresa X entiendan que no pueden demorar la respuesta al requerimiento de los clientes de ser removidos de la lista de correo regular, de correo electrónico, de solicitudes telefónicas o de cualquier otro tipo de lista de mercadeo directo. Si los empleados tardan en el cumplimiento de esta tarea, puede suceder que la lista sea utilizada nuevamente en una campaña telefónica, de correo masivo o de transmisión por correo electrónico y que por lo tanto el requerimiento del individuo no se cumpla. Esto puede causar un grave problema a los representantes de atención al cliente y podría resultar en quejas a la alta gerencia o acciones legales. Esta política hace referencia a la base de datos de la Empresa X y no a listas compradas o alquiladas a terceros. La Empresa X no tiene obligación de notificarle a terceros que proveen listas para una única utilización. Esta política impide los mensajes de correo electrónico no solicitados, de correo regular y las solicitudes telefónicas. Esta política ayudará a la Empresa X a cumplir muchas leyes de privacidad. Desde el punto de vista operacional, es recomendable mantener un registro de los individuos eliminados, tal vez en una base de datos, en caso de una disputa, un error o una solicitud de eliminación no autorizada. La acción descrita en esta política se refiere a veces a "desinscribirse de una lista de correo" sin embargo este término no se utiliza en la política sugerida en vista de que en la mayoría de los casos los individuos nunca se suscribieron.

Políticas Relacionadas: "[Fuente de Material de Mercadeo por Correo Electrónico](#)" e "[Información de Registro del Cliente](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

76. Eliminación de la Información del Cliente o Prospecto

Política: Cuando los clientes o prospectos soliciten que la información acerca de ellos sea eliminada de los registros de la Empresa X, ésta debe rápidamente cumplir este requerimiento a menos que retenga las porciones de los registros de sus transacciones que sean

requeridos por autoridades gubernamentales o que puedan ser necesarios para demostrar el cumplimiento de las leyes y las regulaciones.

Comentario: La intención de esta política de privacidad es demostrar que las organizaciones se preocupan de la privacidad y que están dispuestas a tomar acciones inmediatas en caso de así requerirlo los clientes o prospectos. La eliminación de la información personal del cliente o prospecto evitará que estas personas sean contactadas nuevamente por la organización y que esta información llegue a terceros y que sea utilizada con propósitos no autorizados. Alguna de la información sobre las transacciones debe mantenerse de forma tal que puedan realizarse informes apropiados a las autoridades gubernamentales para detectar fraude o con otros propósitos legítimos de negocio.

Políticas Relacionadas: "[Retención de la Información Personal](#)" y "[Enlaces Entre la Información Privada y la Identificadora](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

77. Bloqueo del Uso de Datos Privados

Política: Los empleados de la Empresa X deben respetar diligentemente el derecho incondicional de los individuos de bloquear los datos acerca de ellos con propósitos de mercadeo, bloquear la venta de estos datos a terceros y eliminar permanentemente estos datos de listas de mercadeo directo.

Comentario: Esta política le da derecho a los individuos descritos en una base de datos o en otro mecanismo de recopilación de datos de borrar el almacenamiento, utilización y distribución de dichos datos. Esta política se aplica a las actividades de mercadeo directo pero puede extenderse a otras áreas como el telemercadeo. Esta política se enfoca en el mercadeo directo porque se trata de una de las principales áreas en las que el cliente siente que su privacidad es violada. Si un individuo solicita que cualquiera de las tres acciones mencionadas en esta política sea llevada a cabo, los empleados deben proceder de la forma más consciente. Pueden existir problemas si la información ya ha sido distribuida a terceros. Algunas organizaciones desearían incluir procedimientos a seguir en caso de que la diseminación de información a terceros ya haya tenido lugar. La idea subyacente dentro de esta política es que los individuos son Propietarios de su información privada.

Políticas Relacionadas: “Registro del Movimiento de Documentos Secretos” y “Distribución de Materiales de Mercadeo”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

78. Compartir Información Personal

Política: La Empresa X no puede vender, alquilar, comerciar, prestar o transferir ninguna información personal de los clientes o prospectos a cualquier otra organización incluyendo, sin limitantes, afiliados, subsidiarias, compañías filiales, casas matrices y socios estratégicos.

Comentario: Esta política hace mención a un vacío existente en muchas leyes y políticas de privacidad. Este vacío permite que las organizaciones que poseen una política de privacidad argumenten que no transfieren información privada a organizaciones externas, pero nunca definen explícitamente el término "organización externa". En lugar, declaran que muchas organizaciones forman parte de su estructura organizacional. Esto les permite compartir la información privada de una manera jamás sospechada ni autorizada por los clientes y prospectos. Por ejemplo, algunos bancos han compartido información privada con compañías aseguradoras cuando ambas pertenecen a la misma casa matriz. Esta política evita este tipo de abusos y permite que todo el mundo sepa que no existe intención de involucrarse en este tipo de prácticas engañosas. Puede añadirse una excepción a esta política en caso de transferencia de información personal a una organización subcontratada. En este caso deberían también añadirse a la política seguridades adicionales acerca de los acuerdos de confidencialidad y controles apropiados.

Políticas Relacionadas: “Transferencia de Datos Personales” y “Compromiso en Acuerdos de Confidencialidad”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

79. Transferencia de la Información sobre Clientes

Política: Si la Empresa X es cerrada, fusionada, adquirida por otra, u ocurre cualquier otro cambio legal en su estructura organizativa, la Empresa X puede

necesitar compartir toda o parte de la información de sus clientes con otra entidad, por lo que éstos deben ser notificados rápidamente.

Comentario: Esta política permite que una organización posea gran flexibilidad en la manera en que maneja su negocio y evita que ciertas oportunidades de negocio sean consideradas inviables porque se haya adoptado previamente una política de privacidad restrictiva. Esta política reconoce implícitamente que los proveedores de sistemas informáticos cambian con regularidad la estructura de sus negocios. Esta política está definitivamente a favor de los negocios y aporta poco en términos de protección al cliente. La protección que provee esta política podría sustentarse si se añadiera otro enunciado al final de la misma tal como “si los clientes objetan esta transferencia, la información no será transferida o utilizada por la otra entidad”. Esta política no permite que la organización venda la información del cliente como un activo independiente y diferente siempre que la venta ocurra durante el proceso de quiebra o de otra manera. Este tipo de venta sería permisible únicamente en caso de que continúen proveyéndose productos o servicios similares.

Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

80. Transferencia de Datos Personales

Política: La Empresa X no debe compartir la información personal sobre sus clientes con otras organizaciones que no sean subsidiarias, empresas subcontratadas o socios estratégicos de negocios, a menos que la Empresa X esté en quiebra, sea fusionada o adquirida por otra.

Comentario: Esta política protege a la organización originaria pero suministra muy poca protección a la privacidad. No es un buen ejemplo de una política de protección de la privacidad. Se basa en las políticas de un gran número de negocios en línea que se eximen de proteger los datos personales en caso de quiebra o venta. Mientras que una organización en algunas jurisdicciones podría adoptar legalmente una política como ésta, debería tener el suficiente soporte de relaciones públicas para defenderse en caso de alegatos acerca de que se trata de un mal ciudadano corporativo que viola deliberadamente los derechos de los clientes y que no se encuentra deseoso de contribuir con los aspectos relacionados con la privacidad. Debería también

aprobarse y disponer de un respaldo más restrictivo para esta política, de forma que una política nueva y más rigurosa pueda ser emitida en caso de que se presenten este tipo de alegatos en contra de la organización.

Políticas Relacionadas: “Transferencia de la Información sobre Clientes” y “Bloqueo del Uso de Datos Privados”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

81. Usos de Datos Personales Después de Una Fusión o Adquisición

Política: Si la Empresa X o cualquiera de sus bases de datos de información personal son vendidas, fusionadas, adquiridas o de cualquier otra manera transferidas a otra organización, esta información no puede ser utilizada para nuevos y no previstos propósitos a menos que los individuos involucrados aprueben estos nuevos usos.

Comentario: Esta política tiene como intención proveer a los clientes y prospectos de una certeza adicional de que su información personal no será utilizada para nuevos y no previstos propósitos que ellos no aprobaran simplemente porque el Custodio de sus datos haya sido fusionado, adquirido, quebrado o cualquier otra forma de cambio en la naturaleza de su negocio. Esta política no solamente se refiere al cambio de Custodio de la información personal sino que también toma en cuenta la venta no autorizada de esta información a otra entidad. Esta política informa a los clientes y prospectos que esta venta o transferencia podría ocurrir y les garantiza que no se le dará nuevos usos a su información como consecuencia de este cambio, a menos que ellos lo autoricen explícitamente. Esta política asume que los usos de los datos personales o privados son explicados en el estatuto de privacidad. Esta política restringe deliberadamente las actividades de la Gerencia de Mercadeo que deseé utilizar la última tecnología para conocer acerca de sus clientes y prospectos. Deberían mencionarse los posibles usos internos en la política que podría ser anunciada en una página web o en un sitio comercial de Internet.

Políticas Relacionadas: “Aplicación de Política de Privacidad” y “Autorización para Inclusión en Sistemas de Datos Privados”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

82. Cambios en la Estructura del Negocio y la Transferencia de Datos Privados

Política: La Empresa X no puede transferir datos privados de los clientes a terceros, sin importar qué tipo de cambios organizacionales experimente.

Comentario: Esta política responde a los clientes de comercio por Internet que se encuentren preocupados de que su información privada sea vendida a terceros para satisfacer obligaciones pendientes de pago del negocio. Esto sería una violación de la política de privacidad a menos que ésta mencione cambios específicos como la quiebra. Esta política es necesaria debido a que es común en el mundo de negocios la práctica de transferencia de datos privados de los clientes como parte de una fusión o adquisición. La política bloquea este tipo de transferencias y elimina cualquier tipo de incertidumbre que podría posteriormente conducir a una disputa legal. Algunas organizaciones intentan eludir sus compromisos previos con la privacidad manifestando que el nombre de la organización será transferido junto con la lista, de forma tal que técnicamente no la están vendiendo a terceros. Sin embargo, este tipo de alegatos le dan un mal nombre a la comunidad de negocios por Internet frente a los que abogan por la privacidad. La política descrita aquí puede ayudar a recobrar parte de la confianza perdida.

Políticas Relacionadas: “Usos de Datos Personales Después de Una Fusión o Adquisición”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

83. Indices de Base de Datos Que Contienen Información Privada

Política: La Empresa X debe actualizar e indexar anualmente todas las bases de datos internas y archivos que contengan información privada y hacer que este índice esté disponible a los empleados y terceros descritos estas bases de datos y archivos.

Comentario: Esta política asegura que las personas que están descritas tengan conciencia de todos los registros computarizados acerca de ellas. Este conocimiento permite que los individuos puedan chequear los registros con fines de exactitud y para revisar la distribución adecuada de esta información privada. Si las personas desconocen la existencia de esta información y dónde se encuentra almacenada, no podrán objetar o ejercer sus derechos en relación con su información. Un índice de todas las bases de datos que contengan información privada es también muy útil

desde el punto de vista del manejo de seguridad de la información, debido a que puede utilizarse para asegurar que la información privada está consistentemente recibiendo la protección que requiere. Sería útil, por ejemplo, para determinar si la información está protegida de forma proporcionada con su sensibilidad sin importar en dónde se almacena, quién tiene acceso a ella, qué forma toma, qué tecnología se utiliza para manejarla y con qué fin se utiliza.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” e “[Inventario de Activos — Información](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

84. Lista de Tipos de Información de Producción Disponibles para Empleados

Política: La Gerencia de Tecnología de la Información debe crear y actualizar anualmente una lista completa de los tipos de información de producción que mantiene la Empresa X, hacer que esta lista esté disponible para todos los empleados e informarles qué tipos de información están a su alcance para su inspección.

Comentario: El propósito de esta política es revelar qué tipos de información posee la organización e informar a los empleados qué tipos de información personal sobre ellos mantiene. Esta política protege la privacidad porque requiere que los empleados estén informados sobre las razones por las que no pueden tener acceso a ciertos datos. A pesar de que esta política puede parecer difícil de implementar, no necesita mucho más allá del establecimiento y mantenimiento de un diccionario de datos de la organización. Los requisitos no son tan agobiantes como parecen, debido a que este diccionario de datos está restringido a la información de producción. Los beneficios de esta política se encuentran principalmente en el área de relaciones públicas y de mejoramiento de la moral del empleado. Esta política también ayudará a las actividades de manejo de los sistemas informáticos, como por ejemplo la planificación de bases de datos y de aplicaciones.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” y “[Diccionario de Datos](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

85. Negativa a Proporcionar Información Innecesaria

Política: No se puede negar ningún beneficio de la Empresa X a la persona que se niegue a suministrar información confidencial innecesaria cuando el departamento legal de la Empresa X haya resuelto todas las disputas acerca de la definición de “información confidencial necesaria”.

Comentario: Esta política evita que los empleados, clientes y otros se vean afectados porque no deseán revelar información confidencial que no es indispensable. Por ejemplo, si un supermercado pregunta acerca del estado civil y esta información no es provista, no se pueden negar el cambio de cheques u otros servicios. Se pueden en cambio negar productos o servicios si la información no revelada es necesaria.

Políticas Relacionadas: “[Mal Funcionamiento del Control de Acceso](#),” “[Resolución de Quejas](#),” y “[Verificaciones de Historia Crediticia de Empleados Potenciales](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

86. Cifrado de Correo Electrónico Privado

Política: Nunca se debe transmitir a través de correo electrónico información descifrada que haya sido catalogada como privada.

Comentario: Esta política evita que la información confidencial sea interceptada por personas no autorizadas. El cifrado descrito en la política puede ser provisto por el usuario o puede ser parte del sistema de correo electrónico. El usuario debe asegurar que se utiliza el cifrado antes de que envíe información confidencial. La política asume que se ha adoptado un sistema de clasificación de datos que define la etiqueta “confidencial”. Esta es una política recomendable porque el correo electrónico no es un método seguro para transmitir ninguna información.

Políticas Relacionadas: “[Envío de Información Secreta Vía Fax — Cifrado](#)” e “[Información Secreta en Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

87. Aviso de Cambio en Política de Privacidad

Política: Los miembros del personal de la Empresa X deben llevar a cabo los pasos razonables para notificar rápidamente a todos los individuos afectados en caso de que exista un cambio sustantivo en sus políticas de privacidad.

Comentario: Esta política asegura que los empleados lleven a cabo los pasos necesarios para notificar rápidamente a todos los individuos afectados en caso de que exista un cambio sustantivo en sus políticas de privacidad. Por ejemplo, una restricción en los derechos de privacidad previamente garantizados, requerirá de una notificación. Esta notificación podría por ejemplo hacerse colocando unas pocas palabras en la página de inicio del sitio web. Esta política tiene como objetivo evidenciar la disposición de la gerencia de notificar a todos los individuos los cambios en su política de privacidad. En realidad, no todos los individuos estarán disponibles debido a cambios de dirección, números telefónicos no listados, direcciones de correo electrónico erróneas, y otras clases de problemas. Con relación a estas clases de dificultades para notificar a los individuos, la política utiliza las palabras "pasos razonables". Esta política requiere la notificación después de efectuado el cambio y permite que los individuos afectados modifiquen su relación con la organización, en caso de que deseen hacerlo como respuesta al cambio en la política. Esta política permite que los individuos notificados acepten o rechacen un nuevo servicio, tal vez a través de Internet con una solicitud que puede realizar este proceso automáticamente.

Políticas Relacionadas: ["Puntos de Recopilación de Datos Personales y la Privacidad"](#) y ["Herramientas de Monitoreo de Sistemas"](#)

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

88. Resumen de Diferencias en Políticas de Privacidad

Política: Cuando la Empresa X modifica la política de privacidad, todos aquellos que se ven afectados y provistos de un resumen con todos los cambios y su posible impacto.

Comentario: Esta política fortalece la confianza del usuario de realizar negocios con un comerciante de Internet. Los clientes y prospectos desean saber cómo será su interacción con una organización en el futuro.

Esta política reduce los temores sobre el posible abuso de los datos confidenciales recopilados por un comerciante de Internet. Esta política indica que el expedidor de la política dará un resumen de las variaciones. Esto facilita las cosas para los usuarios debido a que no tienen que leer de nuevo toda la política para tratar de determinar qué ha cambiado. Esta política se encuentra en completa oposición a las prácticas poco amistosas de algunos comerciantes que esperan que el lector revise su política de privacidad regularmente para determinar por sí mismo si la política ha sido modificada y en caso afirmativo, cómo lo ha sido. Este último acercamiento implica una gran carga para el usuario.

Políticas Relacionadas: ["Importancia de la Política de Privacidad"](#) y ["Aviso de Cambio en Política de Privacidad"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

89. Importancia de la Política de Privacidad

Política: La Empresa X debe asegurar que su política de privacidad se encuentra completa, que no existen excepciones y que hace referencia a todas las interacciones con los clientes sin importar los canales de comunicación, los departamentos involucrados dentro de la Empresa X y qué tópicos abarca esta interacción.

Comentario: Esta política podría parecer innecesaria. Sin embargo, los más recientes abusos de privacidad de los comerciantes de Internet indican lo contrario. Algunas organizaciones de cuidado personal han anunciado una política de privacidad para su sitio web indicando que no compartirán información personal de salud con terceros. También poseen sitios de conversación en línea o cualquier otra facilidad en los que tengan otra política que declara que "cualquier información que un participante transmite o anuncia puede ser utilizada con cualquier fin". Algunos de los visitantes a este sitio pueden haber leído la política del sitio web pero no haber revisado cuidadosamente la referida a los sitios de conversación en línea o demás facilidades. La política de privacidad es un área muy compleja y este tipo de manejos de los comerciantes de Internet únicamente confunden a los participantes y le dan a la industria una mala reputación. Esta política informa a los lectores que existe una sola política y que no tienen que ubicar y leer políticas separadas para diferentes tipos de interacciones con la Empresa X.

Políticas Relacionadas: ["Acceso del Cliente a Información Personal"](#)

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

90. Puntos de Recopilación de Datos Personales y la Privacidad

Política: Todos aquellos puntos en donde se recopilan datos personales para ser utilizados por los sistemas informáticos de la Empresa X deben incluir una copia de la política de privacidad de la Empresa X aprobada por la Gerencia de Seguridad Informática.

Comentario: El propósito de esta política es requerir que los clientes y prospectos estén consistentemente informados acerca de la política de privacidad de la Empresa X. Esta política indica que en cualquier punto en donde se recopilan datos personales, debe existir una declaración sobre privacidad. No todas estas copias sobre la política de privacidad necesitan ser comprensibles. Más bien, la información debe ser diseñada en función de la información recopilada. Esta política evita las disputas que se presentan en diferentes departamentos que mantienen posiciones disímiles acerca de la privacidad. Esta política asume que se ha desarrollado y publicado una política de privacidad corporativa. Igualmente, esta política asume que los empleados saben qué es la información personal.

Políticas Relacionadas: “[Herramientas de Monitoreo de Sistemas](#)” y “[Verificaciones de Historia Crediticia de Empleados Potenciales](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

91. Identidad del Recolector de Información Privada

Política: Tanto el nombre legal del recolector de la organización como la información actual de contacto deben ser revelados en cada punto en donde se recopile información privada.

Comentario: Esta política evita que terceros recopilen información privada sin el conocimiento del usuario. Ciertas organizaciones de mercadeo obtienen información de los navegantes de Internet sin desplegar quienes son las entidades que recopilan la información y sus formas de comunicación. No desplegar el nombre de este tercero y no proveer su información de contacto podría parecerle a muchas personas como un acto deshonesto y reprimible. También debería desplegarse el hecho de que la información está siendo recopilada.

Esta política ayudará a instruir a los diseñadores de sitios web acerca de los tipos de visualización que deben realizar. Si algunos de estos diseñadores consideran que la visualización ordenada por esta política amenaza sus actividades de recopilación de información privada, entonces necesita examinarse más adelante la conveniencia de las actividades de recopilación. La palabra "privada" también necesita una definición cuando la organización adopta esta política. Por ejemplo, si la corriente de información fuera anónima, generalmente no sería considerada como privada, a pesar de que describe actividades de ciertas personas.

Políticas Relacionadas: “[Aviso de Recopilación de Información](#)” y “[Recopilación Furtiva de Información Privada](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

92. Explicación del Requerimiento de Información Privada

Política: Cada vez que los trabajadores o los sistemas informáticos de la Empresa X soliciten información privada, deben revelarse las razones completas y detalladas para recopilarla.

Comentario: Esta política permite al individuo que revela los datos privados tener la información suficiente para tomar esa decisión; por ejemplo, a una persona que solicite pagos de asistencia social del gobierno se le pedirá que suministre información sobre sus ingresos, sus recursos financieros y sus bienes personales sin la cual el gobierno puede rehusarse a proporcionar la asistencia, lo cual puede explicarse al individuo al momento de solicitar la información. Esta política limita las cosas que la organización recolectora puede hacer con la información privada porque los propósitos para solicitarla se revelaron al momento en que la misma se suministró. Algunas organizaciones quizás deseen eliminar de la política las palabras "completas y detalladas" para tener una oportunidad de utilizar la información para otros propósitos en el futuro; sin embargo, no es aconsejable hacerlo porque el uso posterior para propósitos no revelados puede colocar a la organización en una situación difícil en cuanto a las relaciones públicas y a las relaciones con el cliente.

Políticas Relacionadas: “[Declaración Explicativa del Empleado](#)” y “[Conciencia del Usuario Sobre Registros de Violaciones de Seguridad](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos

93. Distribución de Políticas de Privacidad

Política: Todas las políticas internas de privacidad de la Empresa X que un cliente potencial o un cliente pueda necesitar saber deben ser posteadas públicamente o distribuidas periódicamente de algún otro modo a estas mismas personas.

Comentario: Esta política obliga a la gerencia interna a tomar en consideración lo que los clientes potenciales y los clientes necesitan saber sobre la privacidad de los datos que la Empresa X posee. Cualesquiera sean estas políticas, deben ser comunicadas a estas personas para que puedan manejar la información sobre ellos mismos apropiadamente. Es recomendable porque requiere que la gerencia interna ajuste con regularidad sus políticas de privacidad a la par de los cambios en los asuntos que los clientes potenciales y los clientes necesitan saber; por ejemplo, en la medida en que el robo de identidad se convierte en un problema más grave en los años venideros, estas mismas personas necesitarán saber más sobre la forma de protegerse y lo que la organización que adopte las políticas está haciendo para ayudar a prevenir el problema. Generalmente, esto implicaría revisiones periódicas a la política de privacidad posteada. La manera en que muchas instituciones financieras implementan esta política es incluir encartes de papel junto con sus facturas mensuales una o dos veces al año. Las políticas de privacidad de mensajes en los sitios de web y otras ubicaciones públicas también son recomendables.

Políticas Relacionadas:“[Aviso de Cambio en Política de Privacidad](#)” y “[Puntos de Recopilación de Datos Personales y la Privacidad](#)”

Política Dirigida a:Gerencia y personal técnico

Ambientes de Seguridad:Todos

94. Revisión de los Archivos Privados de Usuarios

Política: Cada vez que los administradores autorizados del sistema revisan los archivos de usuario privado para atender emergencias u otras necesidades de negocio, se debe notificar con prontitud al usuario mencionado a menos que se esté llevando a cabo una investigación de presuntos actos criminales o de abuso.

Comentario: La intención de esta política es informar a los usuarios que sus archivos pueden ser revisados y copiados por un administrador del sistema en el

transcurso de las actividades normales del negocio. Algunas organizaciones quizás deseen que se requiera que los administradores obtengan un permiso previo de la gerencia antes de revisar los archivos de usuario privado. Una manera alterna y más conveniente para manejar el asunto de la autorización de la gerencia es requerir que los administradores notifiquen a la gerencia después del hecho. Algunas organizaciones pueden desear limitar la parte sobre notificaciones de la política a los usuarios internos. Esta política brinda una garantía de privacidad poco sólida porque plantea que los administradores solamente verán los archivos del usuario para necesidades justificadas de negocio.

Políticas Relacionadas:“[Acceso a Información Sensible o Valiosa](#),” “[Otorgamiento de Acceso a la Información de la Organización](#),” y “[Privacidad en Correo Electrónico](#)”

Política Dirigida a:Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

95. Modificaciones a la Información Personal

Política: Antes de realizar cualquier cambio en los datos personales de los sistemas de producción de la Empresa X basado en una solicitud del cliente, éste debe suministrar la información anterior correcta.

Comentario: Esta política requiere que los representantes de servicio al cliente confirmen la versión previa de información personal antes de que realicen algún cambio en las bases de datos de los sistemas informáticos de producción. Si un cliente que se encuentra en el otro extremo de una conexión de Internet o de una línea telefónica no puede suministrar la versión previa correctamente, es muy probable que él o ella no sea la persona autorizada para solicitar el cambio. Este control es poco efectivo y debe emplearse junto con otras medidas de seguridad tales como una contraseña específica del cliente o algún otro mecanismo para verificar la identidad de la persona que está solicitando el cambio. Algunas organizaciones permiten que los representantes de servicio al cliente proporcionen ayuda a éste último para que suministre la información previa correctamente, aunque esto reduce la efectividad del control.

Políticas Relacionadas:“[Contraseñas de Servicio al Cliente](#)” y “[Códigos de Identificación para Soporte Técnico](#)”

Política Dirigida a:Personal técnico

Ambientes de Seguridad:Todos

12.01.05 Prevención del Uso Indebido de las Instalaciones de Procesamiento de Información

1. Juegos en los Sistemas de Computación de la Organización

Política: No se pueden almacenar o usar juegos en ninguno de los sistemas de computación de la Empresa X.

Comentario: Esta política establece que no se pueden usar juegos en los sistemas de la Empresa X ya que con frecuencia éstos se descargan de sitios de la web y de los boletines y pueden estar infectados con virus del computador o con caballos de Troya, además de que pueden distraer a los empleados de las tareas que tienen asignadas. Adicionalmente, los juegos pueden crear una atmósfera informal y poco seria que resulta inapropiada y que algunas organizaciones consideran poco profesional. Debido a que con frecuencia los juegos se duplican y se distribuyen ilegalmente, éstos también pueden inadvertidamente exponer a la organización a responsabilidades derivadas del copiado no autorizado de software. Como la mayoría de los juegos se encuentran en los computadores personales, las estaciones de trabajo y otros sistemas pequeños, esta política es particularmente pertinente para los ambientes de sistemas pequeños. Algunas organizaciones querrán ampliar el alcance de la política para incluir software de dominio público, porque es probable que este software también contenga virus, caballos de Troya y funciones no deseadas ni autorizadas. Esta política puede hacerse cumplir a través de gerentes de licencia de software automatizado que impiden la ejecución de software que no ha sido autorizado por la gerencia.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Copias de Software”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

2. Uso Personal de los Sistemas de Computación y de Comunicaciones

Política: El computador y los sistemas de comunicaciones de la Empresa X deben usarse únicamente para propósitos de negocio, salvo que se haya obtenido un permiso especial del gerente del departamento.

Comentario: Esta política brinda una orientación en cuanto al uso personal del computador y de los sistemas de comunicación. Sin esta advertencia, un empleado podría por ejemplo estar dirigiendo encubiertamente su

propia oficina de servicios de computación, manteniendo grupos de apuestas, jugando juegos de computador o haciendo llamadas telefónicas personales de larga distancia en forma desmedida. Cuando se les plantea directamente la realización de dichas actividades, los empleados pueden alegar que tenían entendido que estaba permitido o que se trataba de un beneficio complementario. Como una variación al enfoque normal descrito en esta política, algunas organizaciones permiten el uso cuando es estrictamente personal. Con esta variación, si el uso es para llevar a cabo otra actividad comercial como por ejemplo la venta de seguros como un segundo trabajo, queda prohibido. Otras organizaciones permiten el uso personal durante las horas de menor actividad o durante el horario no laborable del personal. Cualquiera sea la filosofía que adopte la organización, es prudente definir con precisión el término “uso personal”, el cual necesita abordar situaciones tales como las tareas de programación para un curso que se está tomando en una universidad local cuyo propósito es aumentar las habilidades que este empleado utiliza en su trabajo regular. Esta política aplica más al personal interno que a aquellas personas que se suscriben a una operación del proveedor de servicio de Internet o dirigen un centro de computación outsourcing. La persona que debe dar la autorización es un gerente de departamento o quizás un vicepresidente en lugar del Propietario de la información porque esta política se relaciona más estrechamente con el uso que un empleado hace de los sistemas más que con la información. A menos que se emplee un software especial de monitoreo, la supervisión del cumplimiento de esta política puede dificultarse porque los teléfonos móviles, los computadores portátiles y equipos afines se usan con frecuencia en el área fuera de la vista de la gerencia lo cual no quiere decir que se deba descartar. De hecho, la política adquiere mayor importancia como un medio mediante el cual una organización evita responsabilidades por actividades no autorizadas llevadas a cabo con sus sistemas.

Políticas Relacionadas: “Uso Distinto al Empresarial de la Información de la Organización,” “Uso Personal del Teléfono,” “Usos del Sistema de Correo Electrónico,” “Uso Personal de Internet,” y “Juegos en los Sistemas de Computación de la Organización”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

3. Uso Personal Incidental de los Sistemas de Comunicación

Política: El computador y los sistemas de comunicación de la Empresa X deben utilizarse únicamente para propósitos de negocio, salvo que su uso sólo consuma una cantidad insignificante de recursos que de otro modo pudiesen emplearse para propósitos de negocio, no interfiera con la productividad del trabajador y no tenga prioridad sobre otras actividades de negocio.

Comentario: Esta política define el uso personal de los sistemas informáticos del negocio, tales como los sistemas telefónicos, los de correo electrónico y los de discado para el acceso a la Internet además de describir las prácticas imperantes en muchas organizaciones en forma veraz; de igual modo debería compararse con muchas otras políticas que existen sobre el uso personal las cuales son excesivamente rígidas. Por ejemplo, en algunas se prohíbe al trabajador hacer una llamada personal a una niñera para acordar la hora en la que se va a recoger al niño. Esto podría ser contraproducente cuando el trabajador necesite hacer nuevos arreglos para que él o ella pueda quedarse a trabajar sobretiempo. Las restricciones aquí mencionadas sobre el uso secundario permiten el uso personal siempre y cuando se cumplan las condiciones establecidas. Este enfoque responsabiliza a los empleados más que a la gerencia en el control del uso personal.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones,” “Uso Personal del Teléfono,” y “Juegos en los Sistemas de Computación de la Organización”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Uso Personal Razonable de los Sistemas de Computación y de Comunicaciones

Política: El uso personal del computador y de los sistemas de comunicaciones debe ser consecuente con las normas convencionales de conducta cortés y ética.

Comentario: Esta política aclara el significado de uso personal aceptable de los sistemas informáticos de la Empresa X, es deliberadamente flexible en su esencia y no requiere de mayores ajustes, si acaso fueren necesarios, porque las normas convencionales de conducta cortés y ética cambian. Por ejemplo, la transmisión de insultos acalorados y desmesurados es un problema cada vez menos grave en la Internet y este cambio es un

reflejo de una norma de conducta que se ha desarrollado. La palabra "razonable" se empleó para permitir que la gerencia tenga conversaciones confidenciales con los trabajadores sobre su uso personal de los recursos del sistema que estimularía a estos trabajadores a dedicar más tiempo a los asuntos relacionados con el negocio y menos tiempo a los asuntos personales. Esta política funciona en forma óptima si se complementa con controles que midan o bloqueen ciertos usos personales. Por ejemplo, se puede emplear un cortafuego para bloquear sitios específicos en la Web.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Uso Personal Incidental de los Sistemas de Comunicación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

5. Acceso de Usuarios a Internet

Política: Los usuarios que acceden a la Internet con las facilidades de la Empresa X deben estar informados que lo hacen a su propio riesgo y que la Empresa X no se responsabiliza por el material que los usuarios vean, descarguen o reciban a través de la Internet.

Comentario: Esta política informa a los usuarios sobre la posibilidad de que encuentren material ofensivo en la Internet y de que la Empresa X no ha examinado la Internet por ellos. Aun cuando se utilicen varios filtros de software para bloquear sitios censurables de la web y se eliminan mensajes de correo electrónico no deseados, es inevitable que se reciban algunos materiales inaceptables. Estos filtros nunca son perfectos y debido en parte a que la Internet está cambiando con tanta rapidez, no pueden nunca ser configurados de una manera realista para bloquear todo. Esta política informa a los usuarios que este material censurable está en circulación y que ellos no deben hacer a la Empresa X responsable de protegerlos de este material. Con esta política, se pueden evitar las acusaciones en el sentido de que la Empresa X creó un lugar de trabajo hostil o de que fomentó un ambiente de trabajo inaceptable.

Políticas Relacionadas: “Sitios Web No Relacionados con Negocio,” “Control de Tráfico en Internet,” y “Comunicaciones Salientes en Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Clasificación del Uso Aceptable de Internet

Política: El uso de Internet debe clasificarse de la siguiente manera: rojo, en los casos cuando está prohibido en todo momento, amarillo, cuando se permite únicamente con la autorización de los gerentes de departamento o verde, cuando se permite en todo momento.

Comentario: La intención de esta política es describir brevemente lo que está permitido o no en lo referente al uso de la Internet con las facilidades de la Empresa X. Por ejemplo, el grupo rojo podría incluir: divulgar información interna de la Empresa X, descargar software o material con derechos reservados, descargar material ofensivo, usar los recursos de la Empresa X con fines personales y lucrativos, amenazar, hacer comentarios de acoso sexual y molestar a otros usuarios. El grupo amarillo puede abarcar hacer compras personales en la Internet, navegar para estar al día con los intereses personales y administrar las finanzas personales. Finalmente, el grupo verde podría incluir la compra de productos y servicios para la Empresa X, el uso del correo electrónico para asuntos relacionados con el negocio, el desarrollo profesional, la investigación para la Empresa X y la búsqueda de cursos académicos. Este enfoque ofrece un margen poco común de flexibilidad, no sólo porque se pueden añadir con facilidad situaciones adicionales a cualquiera de estas tres categorías, sino también porque la categoría amarilla se deja a discreción de la gerencia local.

Políticas Relacionadas: “[Zonas de Seguridad de la Red](#)” y “[Descargas Grandes desde Internet](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Usos Inaceptables de los Sistemas de Computación y de Comunicaciones

Política: Los suscriptores de los servicios de computación y de comunicaciones no deben emplear estas facilidades para ofrecer sus servicios, vender productos o dedicarse de algún modo a actividades comerciales diferentes a las que están expresamente permitidas por la gerencia de la Empresa X.

Comentario: Esta política limita estrictamente los usos autorizados de los servicios de computación y de comunicaciones ofrecidos por la Empresa X y aplica para aquellas personas que pagan para usar las facilidades de la Empresa X. Asimismo, esta política es aplicable a un boletín electrónico, una oficina de

servicio de computación, una red con valor agregado, un proveedor de servicios de Internet, un proveedor del contenido de la información de la Internet y otras organizaciones similares, muchas de las cuales están preocupadas por el establecimiento de productos y servicios con valor agregado por encima de sus servicios básicos de computación y de comunicaciones y que como mínimo requieren que los productos y servicios mencionados estén autorizados con antelación. Algunas organizaciones quizás deseen añadir una cláusula a esta política que prohíba las actividades con fines caritativos, políticos, religiosos o de otro tipo que no estén relacionadas directamente con el negocio y pueden encontrarla especialmente útil cuando se le niegue a un usuario o a un suscriptor servicios disponibles en el futuro.

Políticas Relacionadas: “[Uso Personal de los Sistemas de Computación y de Comunicaciones](#)” y “[Usos del Sistema de Correo Electrónico](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Uso Personal de Internet

Política: Los sistemas informáticos de la Empresa X no deben usarse para acceder a la Internet con fines personales.

Comentario: Esta política sobre el acceso a la Internet establece claramente que los trabajadores no deben usar las facilidades de la Empresa X para acceder a la Internet. En ningún momento, ésta prohíbe a los trabajadores navegar en la Internet en su propio tiempo y utilizando sus propios sistemas. La razón que tiene la gerencia para adoptar una política como ésta es consecuencia de la cantidad excesiva de tiempo que los trabajadores invierten en la Internet; es principalmente una medida que busca aumentar la productividad al tiempo que reduce el número de situaciones de representaciones no autorizadas de la Empresa X en la Internet, lo cual se logra al separar con claridad los usos relacionados con el trabajo y los usos personales. Esta política puede ser considerada muy estricta por algunas organizaciones por lo que otras opciones incluyen el uso personal de la Internet únicamente después de obtener la autorización explícita de la gerencia o en respuesta a un propósito autorizado de negocio. Algunas organizaciones quizás deseen dar ejemplos de uso personal prohibido, que incluyen dirigir un negocio fuera del trabajo, buscar empleos fuera de la Empresa X, enviar cartas en cadena y solicitar contribuciones para causas políticas o religiosas.

Políticas Relacionadas: “Usos Inaceptables de los Sistemas de Computación y de Comunicaciones,” “Uso Personal de los Sistemas de Computación y de Comunicaciones,” y “Uso Personal del Teléfono”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

9. Uso Personal de los Servicios de Internet de la Organización

Política: Todos los trabajadores que hacen uso de la Internet por razones personales con las facilidades de Internet de la Empresa X deben hacerlo fuera del horario de trabajo.

Comentario: La finalidad de esta política es garantizar que los empleados sepan que no deberían utilizar la Internet por razones personales durante las horas de trabajo. Algunos gerentes están preocupados de que la disponibilidad de acceso a la Internet distraerá a los trabajadores de sus tareas regulares. Esta política permite a los usuarios aprovechar las facilidades de la Empresa X para fines personales y aclara en cuáles casos está permitido; no obstante, la organización debería considerar la utilización de varios productos de monitoreo que permitan a la gerencia determinar la naturaleza del uso de Internet y las horas en las cuales se produce para entonces establecer si dicho uso está en conformidad con la política interna. Asimismo, reconoce que en muchas organizaciones el uso personal de la Internet ya está aceptado como un beneficio complementario y asume que dicho uso ayudará a los trabajadores a adquirir más dominio de esta herramienta lo cual contribuiría indirectamente en los usos de la Internet por razones de negocio. Aquellas organizaciones que deseen adoptar un enfoque más estricto pueden prohibir totalmente el uso personal de la Internet durante el horario de trabajo.

Políticas Relacionadas: “Identificadores Personales de Usuario — Responsabilidad” y “Uso Personal de los Sistemas de Computación y de Comunicaciones”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Tiempo de Acceso Personal a Internet

Política: El acceso del trabajador a la Internet por razones personales mientras utilizan las facilidades de Internet de la Empresa X debe realizarse únicamente después del horario normal de trabajo.

Comentario: Esta política establece un horario después del cual se permite el acceso del personal a la Internet. La existencia del mencionado horario establece con claridad que durante el horario de trabajo los trabajadores deberían emplear los sistemas informáticos sólo para propósitos de negocio y adicionalmente, facilita aún más las rutinas automatizadas de análisis de registro para determinar si durante las horas de trabajo se produce la navegación indebida por la Internet. La política reduce no sólo los requerimientos de ancho de banda de la red durante el día sino que también fomenta la productividad. Además, el hecho de permitir formalmente el uso de los sistemas informáticos de la Empresa X para fines personales es realista y de seguro será apreciado por los trabajadores. Esta política tendría muy poca efectividad en una organización que apoya el horario flexible.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones” y “Uso Personal de Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Restricciones al Uso Personal

Política: El uso personal secundario de los sistemas de computación y de comunicación de la Empresa X debe restringirse a una hora o menos al mes y debe excluir las siguientes actividades: crear o distribuir cartas en cadena, intercambiar información que pudiese considerarse indecente, recibir o reenviar chistes, tener un segundo empleo o buscar otro y participar en juegos de azar o en actividades políticas o benéficas.

Comentario: La finalidad de esta política es establecer con exactitud las expectativas en términos de uso personal para lo cual se define un límite de tiempo específico y una lista de actividades prohibidas. Esta política puede ser especialmente útil cuando se toman acciones disciplinarias en respuesta a usos no autorizados. Probablemente, algunas organizaciones deseen ampliar la lista de actividades prohibidas para incluir las ofertas de servicios o anuncios y la recepción de mensajes de las listas de direcciones del correo electrónico que no están relacionados con el negocio de la Empresa X. No hay nada de particular en el periodo de una hora aquí señalado, pudo haber sido cualquier otro lapso.

Políticas Relacionadas: “Uso Personal de Internet”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad:Todos

12. Identificadores de Usuario Empleados en Actividades Abusivas

Política: Todos los privilegios del sistema asignados a un identificador de usuario que participe en actividades indebidas o delictuales deben ser revocados de inmediato.

Comentario: Esta política evita que continúen las actividades indebidas o criminales. Aunque dificulta al personal el rastreo y el registro de las actividades posteriores de la identificación del referido usuario, tiene la ventaja de que permite tomar acciones inmediatas para reducir los daños. La prioridad de la política es reducir los daños, no reunir las pruebas suficientes para entablar acciones legales. La mayoría de las organizaciones estarían de acuerdo con establecer esta prioridad ya que por lo general no desean la publicidad asociada con un caso en tribunales. Asimismo, permite que se programe una respuesta preparada de antemano en respuesta a conclusiones generadas por un sistema de detección de intrusión (IDS, en sus siglas en inglés) o un software de registro del sistema operativo. Si una rutina de registro del sistema operativo revela que alguien está usando indebidamente un identificador de usuario en particular, como por ejemplo, intentando adivinar las contraseñas, entonces los privilegios del identificador de usuario se pueden inhabilitar inmediatamente. Esta respuesta automatizada puede ser completamente programada de antemano con un IDS de forma que se puedan detectar ataques más complejos y tomar acciones inmediatas. Un ejemplo de esto es el intento de un hacker de aprovechar algunos aspectos vulnerables conocidos que son inherentes al software del sistema operativo. La política señala que la respuesta también puede ser manual. Algunas organizaciones quizás deseen excluir los identificadores de usuario del administrador del sistema debido a que la negación de privilegios a estos usuarios podría dejar fuera del sistema a varias personas autorizadas.

Políticas Relacionadas: “Finiquito de los Privilegios de Acceso” y “Reinicialización de la Contraseña Posterior a la Desactivación”

Política Dirigida a: Personal técnico

Ambientes de Seguridad:Todos

13. Herramientas de Prueba de la Seguridad del Sistema

Política: Los trabajadores de la Empresa X no deben adquirir, poseer, intercambiar o utilizar herramientas de software o hardware que pudiesen emplearse para evaluar o comprometer la seguridad de los sistemas informáticos salvo que la gerencia de Seguridad Informática lo autorice expresamente.

Comentario: Debido a que estas herramientas pueden ser utilizadas con frecuencia para burlar controles, su posesión y uso debe ser restringido estrictamente y debería permitirse únicamente a aquellas personas que necesiten de herramientas poderosas, como los auditores de tecnología de información y los miembros del equipo de ataque de penetración. Aunque estas herramientas están disponibles en el mercado, en la Internet y en los boletines electrónicos, los usuarios de la Empresa X no deben poseerlas. Por la misma razón, los usuarios no deberían tener una base de datos que contenga números activos de serial que se requieren para operar software robado. Hay un problema potencial con esta política pues podría prohibir el uso de utilidades poderosas del sistema. En algunos casos, estas utilidades pueden usarse para burlar mecanismos de control, como los sistemas de control de acceso basados en contraseña para los computadores personales. Para asegurarse de que los usuarios no confundan estas utilidades comunes con los programas cuya intención deliberada es la de violar la seguridad, adjetivos tales como “no autorizado” pueden describir cada tipo de herramienta aquí mencionada. Otra manera de manejar y dar mayor claridad a esta distinción es mediante el uso de una lista de hardware y software autorizados por la organización así como el empleo de textos explicativos adicionales según las necesidades de las personas a quienes va dirigida esta política. Algunos usuarios pueden alegar que nunca tuvieron la intención de utilizar dichas herramientas y que solamente las adquirieron para aprender acerca de los computadores. Por último, excluye el tema sobre la intención del usuario. Si los usuarios tienen las herramientas, serán sujetos a medidas disciplinarias o inclusive al cese de la relación laboral.

Políticas Relacionadas: “Prueba de los Controles del Sistema Informático,” “Divulgación de las Vulnerabilidades del Sistema Informático,” y “Herramientas de Estado de Seguridad del Sistema”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad:Todos

14. Uso Distinto al Empresarial de la Información de la Organización

Política: El uso de la información de la Empresa X para algún propósito que haya sido expresamente establecido por la gerencia debe ser aprobado por escrito por el Propietario designado de la información.

Comentario: Esta política brinda una orientación clara en cuanto al uso de los recursos internos de información de la Empresa X para fines distintos a las actividades normales del negocio. Es recomendable adjuntar una explicación que contenga ejemplos de lo que serían propósitos aceptables e inaceptables del negocio y que exponga una variedad de otros escenarios que están prohibidos. Si un empleado tiene una pregunta sobre algún uso de la información de la Empresa X, esta política señala que él o ella debería preguntar antes de usar la información. Igualmente, debería promover mayor conciencia en el personal sobre el uso de la información interna para propósitos distintos a los establecidos originalmente. Las solicitudes de aclaratoria relacionadas con ciertos usos de la información requerirán que la gerencia defina el significado de uso apropiado. Con el tiempo, la existencia del proceso de autorización puede desalentar prácticas cuestionables que pudiesen crear problemas. Esta política elimina las situaciones en las que un empleado niega tener conocimiento de que no era aceptable usar la información interna para propósitos no comerciales. En diversos procedimientos legales, la falta de notificación al empleado ha sido utilizado eficazmente como defensa.

Políticas Relacionadas: “Uso Personal de los Sistemas de Computación y de Comunicaciones,” “Uso de la Información,” y “Usos del Sistema de Correo Electrónico”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

15. Examen de los Datos Almacenados en los Sistemas

Política: La gerencia de la Empresa X debe reservarse el derecho de revisar toda la información almacenada o transmitida por sus sistemas de computación y de comunicaciones y debe informar a todos los trabajadores que no deben esperar ninguna privacidad asociada con la información que almacenan o envían a través de estos sistemas.

Comentario: Aunque la gerencia tiene la opción de brindarle a sus empleados los mismos derechos de privacidad que disfrutarían al utilizar los servicios de una compañía común como la compañía telefónica, la mayoría de los empleadores está adoptando políticas como las aquí mencionadas. Cualquiera sea la posición que la gerencia asuma, es importante que el estado de privacidad de los datos generados por el empleado en los sistemas de la Empresa X quede claramente especificado. Si los empleados saben que la gerencia puede revisar los datos, es mayor la posibilidad de que se abstengan de usar los sistemas de la Empresa X para actividades no relacionadas con el negocio. Las expectativas del empleado también se deben aclarar para evitar litigios, quejas por parte del empleado y problemas morales.

Políticas Relacionadas: “Derechos de Propiedad Intelectual,” “Monitoreo de Mensajes de Correo Electrónico,” y “Privacidad del Archivo Personal”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

16. Areas de Monitoreo Electrónico

Política: Los trabajadores deben ser informados de que pueden estar sujetos a monitoreo electrónico en áreas donde no hay ninguna expectativa razonable de privacidad mientras se encuentren en las instalaciones de la Empresa X con el objeto de apoyar la medición del desempeño del trabajador y de proteger su propiedad y su seguridad, así como la propiedad de la Empresa X.

Comentario: Esta política informa a los trabajadores que están sujetos a monitoreo electrónico y desestima cualquier objeción que éstos puedan hacer posteriormente manifestando que su privacidad fue invadida sin su conocimiento. Asimismo, estipula claramente las áreas en donde se respetará la privacidad del trabajador. Algunas organizaciones quizás deseen eliminar la frase “donde no hay ninguna expectativa razonable de privacidad” con el fin de no revelar en qué áreas se pueden llevar a cabo actividades ilegales sin ser percibidos. La política establece un acuerdo sobre las áreas en donde el monitoreo electrónico puede emplearse o no.

Políticas Relacionadas: “Monitoreo de Mensajes de Correo Electrónico” y “Recopilación Furtiva de Información Privada”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

17. Discusiones Utilizando Servicios Computacionales y Comunicacionales

Política: Los sistemas internos de computación y de comunicación no deben emplearse como un foro abierto para discutir los cambios en la organización o los asuntos relacionados con la política de los negocios de la Empresa X.

Comentario: Esta política permite que la gerencia censure ciertos usos de los sistemas de computación y de comunicación y, de ser necesario, discipline a los individuos que usan estos sistemas para actividades no autorizadas. Por ejemplo, esto sería importante cuando se producen cambios en el personal. Por razones morales de los empleados, la discusión abierta de tales asuntos no debería encontrarse en los sistemas internos. Una comunicación informando sobre la designación de

un nuevo gerente o miembro del personal estaría permitido según esta política tal y como está escrita porque no implica "discusión". El intercambio libre y abierto de los temas mencionados es lo que algunas organizaciones consideran peligroso y por consiguiente desean prohibirlo. La lista de temas puede ampliarse para incluir nuevos productos, planificación estratégica, fijación de precios, relaciones con el cliente y consideraciones afines. Esta política señala con claridad que los sistemas nombrados no son un lugar apropiado para tratar dichos asuntos.

Políticas Relacionadas: "[Derecho a la Libre Expresión](#)" y "[Uso Personal de Internet](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12.01.06 Reglamentación de los Controles Criptográficos

1. Armamentos en Comercio Internacional

Política: Los usuarios no deben distribuir, directa o indirectamente, software de cifrado ni otras municiones de guerra tal como se define en cualquier reglamentación de comercio internacional de armamentos.

Comentario: Esta política reduce el riesgo de responsabilidad que asume el proveedor de servicios de red o facilidades similares. Otra de sus finalidades se relaciona con el adiestramiento y la conciencia puesto que brinda a los usuarios una oportunidad para aceptar que no distribuirán software de cifrado u otros ítems considerados municiones de guerra. A pesar de su vigencia, esta reglamentación está considerada en líneas generales arcaica y de un valor cuestionable y está siendo cada vez más atacada por limitar la expansión de la industria del software y de los negocios de Internet. Algunas organizaciones requieren que los usuarios manifiesten que cumplirán con esta reglamentación antes otorgarles acceso a las facilidades de la organiza-

ción y algunas veces hasta para la entrada física a las oficinas. Esta política se presentaría en el momento en que un nuevo usuario reciba una perspectiva general de los servicios de red disponibles. Otra manera de manejar este tipo de reconocimiento es hacer que los usuarios firmen un documento declarando que ellos no exportarán a sabiendas, directa o indirectamente, ningún dato técnico, producto o software a algún país restringido sin haber obtenido un permiso del gobierno. Si se produce una distribución ilegal de municiones de guerra, esta política puede ser de utilidad para reducir las multas u otras penalidades a la organización que la adopte.

Políticas Relacionadas: "[Envío de Información Sensible Vía Fax — No Cifrada](#)"

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Medianos y altos

12.01.07 Recopilación de Evidencia

1. Evidencia de Delito o Abuso Informático

Política: Toda la información relacionada con un supuesto uso indebido o delito, incluyendo sin limitantes, la configuración actual del sistema y a las copias de respaldo de todos los archivos potencialmente comprometidos, debe capturarse y almacenarse de

inmediato en forma segura fuera de línea hasta que se otorgue la custodia oficial de la misma a otra persona autorizada o hasta que el asesor legal principal determine que la Empresa X ya no necesita la información.

Comentario: La finalidad de esta política es informar al personal de gerencia de sistemas que cierta información debe capturarse y almacenarse en forma segura hasta que sea requerida por los auditores internos, asesores corporativos, administradores de seguridad y otros. La política permite que se capture y se almacene la evidencia para que pueda ser admisible en el tribunal ya que si la misma permaneciese en el computador implicado por un período de tiempo, existe la posibilidad de que partes no autorizadas pudiesen haberla modificada y por consiguiente sería considerada inadmisible. El proceso de capturar la información debería producirse aunque sólo se sospeche de un problema pues es preferible tener la información y desecharla cuando ya no se necesite, que no tenerla para iniciar acciones judiciales. La política garantiza que se conserva un registro del estado actual de los sistemas y archivos para uso posterior.

Políticas Relacionadas: “Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Fuentes de Evidencia Digital

Política: Para cada sistema de computación de producción, el departamento de Seguridad Informática debe identificar las fuentes de evidencia digital que razonablemente pudiesen ser usadas en un juicio e implementar un proceso normalizado de captura, retención y destrucción similar al que se utiliza para los registros demográficos.

Comentario: Esta política establece un proceso formal para identificar fuentes de evidencia digital antes de que se produzca un incidente de seguridad. Con este enfoque proactivo, los administradores del sistema y otros miembros del personal pueden tomar medidas para manejar en forma apropiada cualquier evidencia digital. Por ejemplo, la evidencia digital potencial necesita pasar a través de un proceso de cadena de custodia mientras que lo que se percibe como registros del sistema de los sistemas de producción no pasarían usualmente a través de este proceso. Si el proceso no fue cumplido desde el momento en que esta información se registró originalmente, tales archivos de registro no pueden ser admitidos en los tribunales como evidencia. Esto depende de las reglas de evidencia dentro de la jurisdicción afectada. Esta política fomenta una nueva conciencia sobre el valor potencial de los registros del sistema, las pistas de auditoría de aplicación, los registros de transacción de bases de datos y otros

registros. Asimismo, garantiza que la información que es potencialmente importante para las investigaciones forenses, se capturará adecuadamente.

Políticas Relacionadas: “Registro de Intentos de Acceso” y “Archivo de Correo Electrónico”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Medianos y altos

3. Divulgación de Información a las Autoridades

Política: Los usuarios deben dar su consentimiento en el sentido de permitir que toda la información que almacenen en los sistemas de la Empresa X se divulgue a las autoridades a discreción de la gerencia de la Empresa X.

Comentario: Esta política informa a los usuarios que no deben tener ninguna expectativa de privacidad con respecto a los sistemas de la Empresa X e igualmente les notifica que no se requerirá de una orden de registro para que los funcionarios de los organismos competentes obtengan acceso a la información que está almacenada en los sistemas de la Empresa X. Probablemente, la gerencia desee revelar cierta información a las autoridades lo cual podría ser pertinente si la gerencia descubriese que sus facilidades de computación se utilizan para realizar actividades ilegales. Esta política maneja las expectativas de los usuarios, asegurándose de que éstos entiendan que no tienen la protección normal de privacidad que se aplica a las compañías de comunicaciones públicas como la compañía telefónica.

Políticas Relacionadas: “Examen de los Datos Almacenados en los Sistemas,” “Divulgación de Información Privada a Terceros,” y “Monitoreo de Mensajes de Correo Electrónico”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4. Información Sobre el Monitoreo del Desempeño

Política: La gerencia no debe utilizar los computadores para recopilar en forma automática información sobre el desempeño de los trabajadores, salvo que los trabajadores mencionados hayan acordado colectivamente que dicha información refleja en forma realista su desempeño en el trabajo.

Comentario: Los contratos sindicales pueden estipular que se tome una decisión colectiva previo a la instalación de tales sistemas de monitoreo de desempeño. Independientemente de la presencia de un sindicato, desde el punto de vista de las relaciones con el personal, es recomendable que los empleados tengan conocimiento de cualquier decisión en relación con la recopilación y el uso de dichos datos. Esta política evita que la gerencia instale y utilice tecnología para el monitoreo del desempeño salvo que se discuta con los empleados y se reconozca su importancia. Además, no interfiere con algunas herramientas de seguridad de los sistemas informáticos como las que permiten que un operador de computación revise en forma subrepticia la información que aparece en la pantalla de un usuario remoto, las cuales son empleadas por el personal del Centro de Atención al Usuario para resolver problemas así como por el personal de seguridad informática para llevar a cabo investigaciones.

Políticas Relacionadas: “[Autorización de Recopilación de Información Privada](#)” y “[Uso de Tecnología Telefónica para Conferencias o Grabación](#)”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

5. Permiso para Monitoreo

Política: La Empresa X no debe monitorear las comunicaciones de un empleado sin su permiso, salvo que el permiso por adelantado pueda modificar alguna conducta específica.

Comentario: Esta política garantiza a los empleados que no están siendo monitoreados sin su conocimiento. Algunas organizaciones querrán ampliar esta política con otras excepciones que sean necesarias para manejar en forma adecuada los sistemas informáticos involucrados. Esto puede incluir los procesos para recuperarse de una infección por virus o para reunir evidencia de ingresos no autorizados a los sistemas. Esta política cubre únicamente a los empleados y no al personal temporal, consultores, contratistas, socios estratégicos de negocio u otros terceros. Si estas otras categorías de individuos deben incluirse, entonces se debe usar la palabra "trabajadores".

Políticas Relacionadas: “[Monitoreo de Mensajes de Correo Electrónico](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

6. Monitoreo de las Comunicaciones de los Empleados

Política: La Empresa X no debe participar en el monitoreo general de las comunicaciones de los empleados, salvo que exista una necesidad justificada de negocio que no pueda ser satisfecha por otros medios, el empleado mencionado no está disponible y el factor tiempo sea crucial en una actividad de negocio, exista una causa razonable para sospechar que se está produciendo una actividad delictiva o una violación a la política o el monitoreo sea requerido según la ley, el reglamento o los acuerdos con terceros.

Comentario: Esta política informa a los empleados que sus comunicaciones pueden ser monitoreadas en ciertas circunstancias e igualmente garantiza a los empleados que no existe un proceso de monitoreo general y que el derecho a monitoreo se usará con criterio y únicamente cuando exista una necesidad justificada de negocio. La política incluye solamente a los empleados y no al personal temporal, consultores, contratistas, socios estratégicos de negocio u otros terceros. Una necesidad justificada de negocio puede abarcar una variedad de problemas técnicos como la recuperación de una infección por virus.

Políticas Relacionadas: “[Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

7. Monitoreo o Grabación de Conversaciones Telefónicas

Política: Las conversaciones telefónicas del trabajador de la Empresa X no deben ser monitoreadas o grabadas a menos que se escuche claramente el tono de beep cuando se realice el monitoreo.

Comentario: Una disposición que permita el monitoreo no anunciado para impedir o investigar actividades ilegales se puede agregar a esta política como una excepción. De conformidad con algunos estatutos de interceptación de líneas telefónicas, esta política requiere que las partes de una conversación sean informadas de que un tercero está escuchando o grabando la conversación. De igual modo, requiere que las conversaciones telefónicas no privadas sean entendidas claramente como tales por ambas partes y que los empleados que están grabando sus propias conversaciones con terceros informen a éstos últimos sobre esta actividad.

Políticas Relacionadas: “Monitoreo del Desempeño”

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

8. Confidencialidad de la Información de las Investigaciones Internas

Política: Todas las investigaciones que se lleven a cabo de supuesta conducta indebida o delictiva debe mantenerse estrictamente confidencial para preservar la reputación de la parte sospechosa hasta que se formulen los cargos o se tomen las medidas disciplinarias correspondientes.

Comentario: Aparte del objetivo aquí señalado, esta política reduce la probabilidad de que la Empresa X esté sujeta a demandas por difamación; la intención es más bien definir claramente el punto en que se permite revelar la información sobre las investigaciones relacionadas con los empleados. Un aspecto positivo es que las investigaciones que no conlleven a acciones legales o medidas disciplinarias no serán nunca reveladas. Si el empleado y sus compañeros de trabajo nunca tuvieron conocimiento de la investigación, aquél puede mantener su prestigio y buena reputación. Si el empleado descubrió que había en proceso una investigación que posteriormente resultó inadecuada, él o ella puede molestarse o, inclusive, separarse pronto de la organización. Si los compañeros de trabajo se enterasen de una investigación que no se materializa, entonces la reputación del acusado resultaría perjudicada sin ninguna necesidad.

Políticas Relacionadas: “Clasificación de Datos en Cuatro Categorías,” “Investigación de Delito Computarizado,” y “Transferencias de Trabajadores”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

9. Investigaciones Policiacas o Legales

Política: Los trabajadores de la Empresa X no deben revelar ninguna información interna de la Empresa X a través de ningún mecanismo de comunicaciones, a menos que hayan establecido la autenticidad de la identidad del individuo y la legitimidad de la investigación.

Comentario: Esta política evita la ingeniería social en donde los atacantes se hacen pasar por miembros de los organismos de seguridad competentes. Tal farsa o engaño ocurre con frecuencia y en ocasiones con éxito.

Si un hacker que se hace pasar por un funcionario del gobierno logra obtener información sobre las configuraciones del sistema de información de la organización, de sus problemas anteriores de intrusión y de los gerentes de importancia en la toma de decisiones, puede ser de gran utilidad en un ataque posterior. La política señala que no todas las personas que manifiesten ser funcionarios de los organismos de seguridad lo sean verdaderamente; sin embargo, las maneras específicas para establecer la identidad del solicitante y la legitimidad de la investigación no están establecidas deliberadamente porque varían de acuerdo a la jurisdicción y al tipo de investigación. En muchos casos, se puede hacer una llamada telefónica de confirmación al director del organismo de seguridad correspondiente para verificar la identidad de la persona que está realizando las indagaciones. Las placas de identificación pueden ser examinadas si el contacto se efectúa en persona. La legitimidad de la solicitud se puede establecer a través de una orden judicial o cualquier otro documento legal parecido.

Políticas Relacionadas: “Divulgación Telefónica de Información” y “Solicitudes de Información Organizacional”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

10. Participación en Procedimiento Legal

Política: Cualquier empleado de la Empresa X que reciba una citación o que sea llamado para testificar frente a un jurado o una agencia gubernamental, debe notificar este hecho por escrito al asesor legal en jefe.

Comentario: Esta política alerta al departamento Legal acerca de una citación para testificar antes de que ocurra. El departamento Legal podría tomar una acción evasiva como por ejemplo presentar una moción para posponer la comparecencia o para presentar una objeción formal. También pueden aconsejar a la persona que será citada de forma tal que se minimice el perjuicio contra la Empresa X. Esta política es una instancia específica que forma parte de un objetivo global para controlar el flujo de información confidencial acerca de las operaciones internas o de las actividades históricas de una organización.

Políticas Relacionadas: “Infracción de la Ley” y “Manejo de Mensajes de Correo Electrónico”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

11. Provisión de Información en Procedimientos Legales

Política: Los empleados no deben suministrar ningún informe de la Empresa X ni copias de él a terceros fuera de la Empresa X ni a funcionarios gubernamentales, en respuesta a una citación o de cualquier otra manera, ni deben testificar acerca de hechos que conocieron mientras desempeñaban sus cargos en la Empresa X, a menos que previamente se haya obtenido autorización del asesor legal en jefe.

Comentario: Esta política evita que los empleados simplemente entreguen documentos internos u ofrezcan información interna con la falsa creencia de que estaban obligados legalmente a hacerlo. Estas solicitudes de información pueden ser efectuadas por el asesor legal de la parte opositora y pueden no ser necesarias. La divulgación de esta información podría además dañar la posición de la Empresa X en una demanda que se encuentre en la corte o que eventualmente vaya a la corte.

Políticas Relacionadas: “[Información de Asuntos Legales](#)” y “[Moratoria en Destrucción de Datos](#)”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

12. Contactos con Autoridades Judiciales

Política: El personal técnico de sistemas informáticos no debe contactar a la policía ni a ningún otro miembro de la comunidad de justicia criminal con relación a algún problema que se le presente en los sistemas informáticos, a menos que tengan autorización del director del departamento Legal.

Comentario: Esta política limita el reporte de problemas de seguridad informática a la comunidad de justicia criminal. Los miembros del personal técnico pueden estar equivocados acerca de un problema, tener demasiadas tensiones, o guardar resentimiento hacia la gerencia. Reportar un problema a la comunidad de justicia criminal también podría conducir a problemas de relaciones públicas que la organización preferiría evitar. Las agencias de justicia criminal a menudo exigen un mínimo de requisitos antes de abrir un caso. El director del departamento Legal puede ayudar al personal técnico a determinar si archiva un reporte o si el hecho en cuestión efectivamente ocurrió y si existe suficiente evidencia. En lugar de dirigirse al director del

departamento Legal, los miembros del personal técnico pueden acudir para obtener la autorización a la gerencia de Seguridad Informática. Esta política asume que la organización no posee un equipo de respuesta computarizada en casos de emergencia altamente desarrollado con procedimientos documentados y adiestramiento en profundidad. Si éste existe, esta política estaría generalmente cubierta dentro de esa documentación.

Políticas Relacionadas: “[Interferencia con Reportes de Violaciones y Problemas](#)” y “[Cumplimiento de la Privacidad](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

13. Reportes Sobre Situación de la Investigación

Política: El estatus de las investigaciones sobre seguridad informática debe ser comunicado a la gerencia únicamente por el jefe de la investigación o por el representante de la gerencia dentro del equipo de investigación.

Comentario: Esta política evita que la gerencia reciba informes inexactos o innecesariamente alarmantes. Después de una intrusión o de cualquier otro problema de seguridad informática, muchas personas podrían aparentar como si supieran acerca del incidente cuando en realidad no se han visto directamente involucradas en él. Esto puede llevar a confusión dentro del personal, problemas en la política interna y costos excesivos. Esta política define quién transmite la información acerca del estatus de una investigación. La documentación acerca del camino a seguir asegura asimismo que los miembros del equipo gerencial no reaccionen o tomen una medida inadecuada en base a los comentarios de personas que no saben qué es lo que está sucediendo. Esta política también asegura que los detalles acerca de la investigación sean revelados únicamente a aquellas personas que necesitan conocerlos. Esto reducirá las probabilidades de que se presenten calumnias, libelos, difamaciones y otros problemas legales.

Políticas Relacionadas: “[Análisis de Violaciones y Problemas](#)” y “[Verificación de Cumplimiento de Seguridad Informática](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

14. Información Sobre Investigaciones de Delitos Computarizados

Política: Toda evidencia, idea e hipótesis acerca de delitos de computación que haya sufrido la Empresa X, incluyendo posibles métodos de ataque e intenciones de ataque, debe ser comunicada al asesor legal interno de la empresa y tratada como información restringida y legalmente privilegiada.

Comentario: El objetivo de esta política es restringir severamente el acceso a información acerca de crímenes de computación que haya sufrido la Empresa X. Esto puede evitar que la Empresa X reciba publicidad negativa, que se desplomen los precios de sus acciones y cualesquiera otros efectos adversos como consecuencia de divulgaciones inapropiadas. Cuando la información se encuentra legalmente privilegiada, también está protegida de ciertas clases de recopilación de información, como por ejemplo la divulgación. Esta política ayuda a que la información acerca de crímenes de computación sea manejada por un número restringido de gerentes y de personal técnico de la organización a pesar de que exista una demanda legal en proceso. Esta política también enfatiza el hecho de que este tipo de información es sumamente sensible y debe ser distribuida únicamente a aquellos que tienen la necesidad de conocerla. Esta política minimiza las posibilidades de que voceros de la Empresa X ofrezcan teorías sin fundamento acerca de intenciones de perpetración o métodos de ataque a los medios de comunicación, exponiendo a la Empresa X a alegatos por calumnia o difamación. La palabra "interno" puede ser eliminada de la política si la organización tiene únicamente asesoría legal externa.

Políticas Relacionadas: ["Divulgación de Ataques a Sistemas de Computación"](#) y ["Reportes Centralizados de Problemas"](#)

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

15. Proceso de Análisis Forense

Política: Todo análisis o investigación en el que se utilicen medios de almacenamiento de datos que contengan información que podría en algún momento convertirse en evidencia importante para un juicio sobre un delito o abuso de computación, debe llevarse a cabo con una copia en lugar de utilizar la versión original.

Comentario: Esta política evita que se modifique la copia original que contiene evidencia importante. Si el original es modificado de alguna manera, la parte opositora en la corte puede alegar que también se han hecho otros cambios. Los investigadores por lo general utilizan programas especializados que pueden hacer una copia de todo el disco duro, incluyendo los archivos eliminados, fragmentos de archivos actualizados, porciones de mensajes electrónicos eliminados y contenidos borrados de la memoria cache de un buscador en Internet. Esta política se aplica a otros medios de almacenamiento de datos como los discos flexibles y los cartuchos magnéticos ópticos. Ciertos medios de almacenamiento de datos como los CD-ROM no pueden ser modificados sin equipo especial. Inclusive en estos casos es recomendable utilizar una copia para evitar cualquier alegato o alteraciones en la evidencia. El medio que contenga almacenados los datos originales debe ser guardado bajo llave y debe establecerse una cadena documentada de custodia.

Políticas Relacionadas: ["Destrucción de Mensajes de Correo Electrónico"](#) y ["Evidencia de Delito o Abuso Informático"](#)

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

16. Investigaciones de Seguridad Informática

Política: Todas las investigaciones internas de la Empresa X sobre incidentes de seguridad informática, violaciones y problemas, deben ser conducidas por personal adiestrado por la gerencia de Seguridad Informática.

Comentario: Esta política evita que los administradores del sistema, gerentes de departamento y otros puedan conducir sus propias investigaciones de seguridad informática. No solamente pueden violarse las leyes sobre privacidad sino que puede ser destruida importante evidencia como consecuencia de un mal manejo de la información. Esta política establece que este tipo de trabajo es altamente especializado y que debe ser realizado por especialistas. Esta política es consistente con el surgimiento de la computación forense. A pesar de que esta política parezca inocua, puede ser muy útil para el especialista en seguridad informática desde el punto de vista de la política interna. El adiestramiento específico requerido no se establece en esta política deliberadamente debido a que el personal técnico disponible para este trabajo y la naturaleza específica del mismo, variará de investigación en investigación.

Políticas Relacionadas: “Revisión de los Archivos Privados de Usuarios” y “Problemas por Accesos No Autorizados”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

17. Equipos de Investigación de Seguridad Informática

Política: Cualquier persona que sea amiga personal o conocida de un sospechoso en una investigación, no debe formar parte del equipo de investigación sobre incidentes de seguridad informática.

Comentario: Esta política evita conflictos de interés, como por ejemplo lealtades personales, que interfieran en las investigaciones. Aquellos miembros del equipo de investigación que conozcan a los sospechosos pueden deliberadamente ignorar la evidencia, malinterpretarla, destruirla, tergiversar el estado de la investigación o interferir en cualquier otra forma con la investigación. Esta política asume que se utilizarán investigadores internos y funciona mejor cuando se aplica a organizaciones grandes. En el caso de organizaciones pequeñas, es difícil encontrar personas que posean los requisitos técnicos para llevar a cabo las investigaciones y que no conozcan personalmente a los sospechosos. En este caso sería conveniente contratar a consultores externos para obtener resultados confiables. Las organizaciones pequeñas pueden añadir una frase a esta política que se refiera al uso de consultores externos con este propósito.

Políticas Relacionadas: “Investigaciones de Seguridad Informática” y “Detalles de Investigaciones de Intrusos”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

18. Investigaciones Internas y Solicitudes Oficiales

Política: Todos los empleados de la Empresa X deben testificar o responder a preguntas relacionadas con investigaciones internas cuando el asesor legal en jefe les indique hacerlo.

Comentario: Esta política pretende informar a los empleados que se espera su apoyo y cooperación en todas las investigaciones internas y averiguaciones oficiales. Esta política tiene como propósito enfatizar la expectativa de que este tipo de soporte y cooperación

forma parte de su trabajo. Esta política evita la tentativa de algunos empleados de proteger a otros de medidas disciplinarias o del despido. Los empleados siempre pueden alegar que desean guardar silencio acerca del asunto que se está investigando o del que se les está preguntando. Esto conducirá generalmente a medidas disciplinarias que podrían incluir el despido. Esta política no viola la ley en algunas jurisdicciones con relación al hecho de guardar silencio si el testimonio podría inculpar a la persona. En la mayoría de los casos este tipo de investigaciones no tiene lugar en la corte por lo que generalmente no aplica el derecho a guardar silencio.

Políticas Relacionadas: “Participación en Procedimiento Legal” y “Reportes Sobre Situación de la Investigación”

Política Dirigida a: Usuarios finales

Ambientes de Seguridad: Todos

19. Detalles de Investigaciones de Intrusos

Política: Los detalles acerca de investigaciones actuales sobre intrusiones en sistemas informáticos no deben enviarse a través del correo electrónico ni deben almacenarse los archivos que describen una investigación actual en sistemas potencialmente interceptables, o en una red en la que puede esperarse que sean vistos por intrusos.

Comentario: Esta política evita que los atacantes puedan averiguar cómo están siendo investigados y actuar para evadir a aquellas personas que intentan sacarlos de los sistemas involucrados. Los atacantes pueden y han llevado a cabo este tipo de vigilancia, como por ejemplo interceptar los mensajes de correo electrónico de usuarios específicos, como los administradores del sistema. Si los violadores poseen los detalles de la investigación, no solamente es probable que destruyan evidencia sino que también tomen acciones evasivas que les permitan retardar el momento en que se logre evitar que entren nuevamente en los sistemas informáticos de la organización. Si la información sobre la investigación es cifrada, en algunos casos puede ser enviada en forma segura a través del correo electrónico o almacenada en lugares en donde los atacantes la puedan encontrar. Sin embargo, generalmente es recomendable mantener esta clase de información lejos de los sistemas afectados. Esto se debe a que la información debe ser descifrada en algún momento para poderla utilizar y en este punto puede ser vista por los intrusos. Por otra parte, si alguno de los

investigadores comete un error, y se equivoca al cifrar la información, podría entonces ser accesible a alguno de los intrusos.

Políticas Relacionadas: “[Informes de Violaciones y Problemas](#)” y “[Evidencia de Delito o Abuso Informático](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

12.02 Revisión de Políticas de Seguridad y Cumplimiento Técnico

12.02.01 Cumplimiento de la Política de Seguridad

1. Cumplimiento del Discado Telefónico

Política: Las conexiones telefónicas discadas a sistemas internos y redes deben ser revisadas por el departamento que hace la instalación y cualquier desviación de las normas internas publicadas debe ser previamente aprobada por la gerencia de Seguridad Informática.

Comentario: Además de controlar el acceso telefónico no autorizado, esta política reduce el trabajo de la gerencia de Seguridad Informática. Esta política transfiere la responsabilidad de verificar la conformidad con las normas internas a la gerencia de los departamentos locales. Las conexiones telefónicas son tan comunes que por lo general es mejor manejarlas localmente. En la era de la computación descentralizada y distribuida, la gerencia local es a menudo la única rama de la gerencia que puede ejercer control sobre los cambios hechos a los sistemas. Esta política asume que ya existen normas internas que definen cómo establecer conexiones seguras. La existencia de estas normas también reducirá significativamente el trabajo de aprobación de conexiones telefónicas requerido por la gerencia de Seguridad Informática. Debido a que las líneas de conexión son a menudo utilizadas por los violadores y otras partes no autorizadas para conseguir acceso a la red, esta política responde a una de las más comunes vulnerabilidades en los sistemas pequeños.

Políticas Relacionadas: “[Conexiones Discadas](#)” y “[Acceso Remoto de Terceros](#)”

Política Dirigida a: Usuarios finales y personal técnico

Ambientes de Seguridad: Todos

2. Responsabilidad por Cese de Trabajador

Política: En el caso de que un empleado, consultor o contratista termine su relación con la Empresa X, el gerente inmediato del empleado debe asegurarse de que devuelva toda la propiedad que estaba en su custodia

antes de que abandone la Empresa X, debe notificar a todos los administradores que manejan las cuentas del computador y de comunicaciones utilizadas por el empleado tan pronto como sea conocida su terminación en el cargo y finalizar todos los privilegios relacionados con su trabajo en el momento en que tenga lugar la terminación.

Comentario: El propósito de esta política es informar a la gerencia específica que debe llevar a cabo determinadas acciones relacionadas con los sistemas en el momento en que el empleado abandona una organización. Estas acciones deben ser tomadas a pesar de que haya finalizado el proyecto de un consultor o contratista. Los empleados disgustados que han sido despedidos pueden hacer daño significativo a los sistemas informáticos. Son de particular cuidado aquellos empleados que tienen acceso a computadores o sistemas de comunicación y que están en una posición importante de confianza. En el caso de esta clase de empleados de confianza, algunas organizaciones podrían querer desarrollar una política independiente con requisitos más estrictos como escoltarlos fuera del edificio en el momento de la terminación. Es recomendable la preparación anticipada en casos específicos de terminación, incluyendo consultas con la asesoría legal interna y con la gerencia de Recursos Humanos.

Políticas Relacionadas: “[Devolución de Propiedad al Cesar Empleo](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

3. Planes Divisionales para el Cumplimiento de la Seguridad Informática

Política: La gerencia de cada una de las divisiones de la Empresa X debe preparar un plan anual de forma que sus sistemas de computación y de comunicaciones estén conformes con sus políticas y normas publicadas.

Comentario: Esta política requiere que la gerencia media elabore planes específicos por escrito en los que se reflejen las formas en las que mejorarán la seguridad informática. Para aquellas organizaciones que están comenzando a considerar seriamente la seguridad informática, una política como ésta puede ayudar a comunicar a la gerencia media que debe darle importancia a la seguridad informática. Al exigirle a la gerencia media que elabore planes e informes periódicos en los que se refleje el proceso de estos planes, esta política puede ser una vía importante de lograr que la gerencia media cumpla. Esta política asegura que la gerencia de sistemas distribuidos enfocará adecuadamente la seguridad informática. Es particularmente útil en aquellas organizaciones fuertemente dependientes de las redes de área local, sistemas departamentales, computadores personales, sistemas cliente-servidor y equipo similar. La referencia a "división" puede ser reemplazada por "departamento", "unidad", "subsidiaria" o cualquier otra clase de agrupación organizacional.

Políticas Relacionadas: "Planes de Seguridad Informática"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

4. Normas de Implantación de Controles

Política: La gerencia debe implementar controles de los sistemas informáticos de forma consistente con las prácticas de negocios generalmente aceptadas y con la criticidad, valor y sensibilidad de la información que procesa.

Comentario: Esta política informa a la gerencia que debe implementar controles que sean consistentes con lo que una corte consideraría como de "legítima diligencia". Esta política reducirá el riesgo de la gerencia de adoptar controles inadecuados debido a que específicamente reconoce la necesidad de este tipo de controles, a pesar de que los controles en sí mismos todavía no se hayan dispuesto. Si una organización realiza esta acción, corre el riesgo de ser acusada de negligencia, rompimiento de la obligación fiduciaria, de dejar de utilizar las medidas de seguridad que tienen otras organizaciones dentro del mismo negocio, de dejar de ejercer el control esperado de un profesional de computación o de fallar al actuar frente a una notificación como el compromiso de la seguridad. La existencia de una política publicada ha sido un factor importante en algunos casos en la corte. Al reflejar el hecho de que cada organización tiene sus propias

necesidades, esta política establece que los controles deben adaptarse al ambiente de negocios de la organización.

Políticas Relacionadas: "Corrección de Registros de Negocios," "Protección de la Información," "Variaciones Respecto de Prácticas de Control Generalmente Aceptadas," "Revisión de los Controles de los Sistemas Informáticos — Independiente," y "Normas de Seguridad Informática Específicas a Cada Industria"

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

5. Variaciones Respecto de Prácticas de Control Generalmente Aceptadas

Política: La gerencia debe revelar las variaciones que perciba de las prácticas generalmente aceptadas en los sistemas informáticos de control y es igualmente responsable de llevar a cabo rápidamente la acción correctiva.

Comentario: Esta política informa a la gerencia que debe percibir las variaciones con relación a la norma de debido cuidado y que lleve a cabo los pasos para corregir estas variaciones. En este sentido, la palabra "variaciones" se refiere no solamente a aquellas situaciones en las que están ausentes las normas de debido cuidado, sino aquellas circunstancias en las que la organización no cumple con controles previamente especificados o implementados. En muchas organizaciones, los auditores internos tienen como función investigar acerca de estos asuntos. Algunas veces este trabajo es responsabilidad de auditores externos o consultores especiales. La gerencia es responsable de vigilar e implementar controles internos apropiados.

Políticas Relacionadas: "Normas de Implantación de Controles" y "Normas de Seguridad Informática Específicas a Cada Industria"

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

6. Evaluaciones de Riesgo de los Sistemas

Política: Cada unidad organizacional dentro de la Empresa X que maneje sus propios computadores o redes debe llevar a cabo una evaluación anual de riesgo relacionado con la seguridad de estos sistemas para posteriormente certificar que se han implementado las medidas de seguridad apropiadas.

Comentario: Esta política delega la responsabilidad de llevar a cabo evaluaciones regulares de riesgo a las unidades organizacionales distribuidas, tales como departamentos, divisiones o subsidiarias que manejan sistemas informáticos locales. Esta política establece que la seguridad informática también es responsabilidad de la gerencia y no solamente de un grupo centralizado de seguridad informática. Mientras que las evaluaciones anuales de riesgo son requeridas para cada unidad que maneja sistemas informáticos, un grupo centralizado de seguridad informática, un grupo auditor de tecnología de la información o una organización independiente de consultoría, deben llevar a cabo evaluaciones periódicas de riesgo independientes de estos sistemas informáticos. El grupo centralizado de seguridad informática debe realizar asimismo evaluaciones de riesgo de los recursos manejados en forma centralizada como las redes. A pesar de que algunos piensen que esto introduce un

conflicto de intereses, las unidades distribuidas no son los únicos grupos que evalúan la seguridad de los sistemas distribuidos. El hecho de que los grupos distribuidos evalúen su propia seguridad es solamente un paso en el manejo responsable de la seguridad. Los grupos distribuidos no pueden manejar la seguridad informática de una manera efectiva o eficiente si no comprenden cuáles son los riesgos involucrados. Esta política puede sustentarse en una guía para llevar a cabo evaluaciones de riesgo elaborada por la unidad centralizada de seguridad informática.

Políticas Relacionadas: “[Excepciones a las Políticas](#)” y “[Evaluación de Riesgo de Seguridad Informática en Toda la Organización](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Medianos y altos

12.02.02 Verificación de Conformidad Técnica

1. Auditorías de Respaldo de Producción

Política: La gerencia de Auditoría Interna debe realizar una revisión anual y pruebas aleatorias de los procesos de respaldo de los sistemas de producción.

Comentario: Esta política alienta a los administradores del sistema y a los operadores de computadores para que le presten atención a la importante área de respaldo de la información computarizada. La existencia de esta política enfatiza la importancia de efectuar diligentemente el respaldo de la información todos los días del año. Estos miembros del personal técnico saben que cada vez que se realiza el respaldo están creando registros extensos de información. Esta política también se aplica a los usuarios finales, en caso de que estén a cargo de realizar respaldos de los sistemas de producción. Los sistemas de producción generalmente no se ejecutan en los computadores portátiles sobre los cuales tienen control los usuarios finales, y por lo tanto esta política no impactaría a la comunidad de usuarios finales.

Políticas Relacionadas: “[Revisión del Respaldo](#)” y “[Archivos de Sitios Web y Comerciales](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

2. Evaluaciones de Riesgo de la Seguridad de Sistemas Informáticos

Política: Deben realizarse al menos una vez cada dos años evaluaciones de riesgos de seguridad para los sistemas informáticos que manejan información crítica y aplicaciones de producción críticas, y todas las considerables mejoras, actualizaciones, conversiones y demás cambios asociados con estos sistemas o aplicaciones, deben estar precedidas de una evaluación de riesgo definida en el manual de Seguridad Informática.

Comentario: Esta política requiere que el personal realice evaluaciones de riesgo antes de que se hagan modificaciones considerables a los sistemas informáticos que manejan información crítica o a las aplicaciones de producción críticas. Esta política asume que la organización ya ha priorizado sus sistemas informáticos en función a su criticidad para la organización. Esta política también asume que se ha definido una metodología para llevar a cabo las evaluaciones de riesgo en otro documento interno como el Manual de Seguridad Informática. La metodología exacta para la evaluación de riesgo no es especificada en forma deliberada en esta política. Esto permite que dicha metodología evolutive en el tiempo sin la necesidad de modificar esta política. En muchos casos, el tipo de evaluación de riesgo también variará de acuerdo con las circunstancias. Por ejemplo, si una evaluación de riesgo fue realizada en una aplicación hace seis meses, entonces únicamente se requerirá una actualización

abreviada de la evaluación anterior. Si por el contrario nunca se ha hecho una evaluación de riesgo, se requerirá una evaluación a gran escala.

Políticas Relacionadas: “[Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones](#)” y “[Planes de Seguridad Informática](#)”

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos

3. Evaluación de Riesgo de Seguridad Informática en Toda la Organización

Política: Cada año la gerencia de Seguridad Informática debe dirigir o manejar a un grupo independiente que lleve a cabo una evaluación a lo largo de toda la organización y genere un informe como resultado de este proyecto en el que se encuentre una descripción detallada de los riesgos de seguridad informática que está enfrentando la organización, con recomendaciones específicas para prevenir o mitigar estos riesgos.

Comentario: Esta política requiere que la gerencia de Seguridad Informática identifique anualmente las amenazas importantes, recientes desarrollos y pasos a seguir. La seguridad informática es un campo complejo y es importante que aquellas personas que trabajan en él

restablezcan las prioridades periódicamente. Sin esta política, los recursos de seguridad informática pueden ser utilizados en atender situaciones que no tienen mucho impacto. Algunos esfuerzos de seguridad informática se enfocan solamente en los virus, planes de contingencia y sistemas de control de acceso, mientras que hay mucho más en relación con la seguridad informática que requiere atención urgentemente. Una evaluación anual de riesgo identificará cuáles son estas tareas adicionales. En vista de que cada organización es diferente, los pasos a seguir deben adecuarse a cada una de ellas. Para poder llevar a cabo este proceso de adaptación o planificarlo, debe realizarse una evaluación de riesgo. Esta evaluación constituye también un muy importante documento de referencia cuando se elaboran políticas, normas, procedimientos, arquitecturas o cualquier otro material de infraestructura organizacional. La política no especifica deliberadamente el método para una evaluación de riesgo debido a que puede cambiar en el tiempo de forma que se dé un mayor entendimiento respecto de la situación real.

Políticas Relacionadas: “[Análisis de Violaciones y Problemas](#)” y “[Evaluación del Riesgo en los Sistemas de Producción](#)”

Política Dirigida a: Gerencia

Ambientes de Seguridad: Todos

12.03 Consideraciones sobre Auditoría de Sistemas

12.03.01 Controles de Auditoría de Sistemas

1. Atributos de la Integridad de la Información

Política: Dentro de lo posible, la gerencia debe notificar periódicamente acerca de la exactitud, oportunidad, relevancia y demás atributos de integridad informática que describen a la información utilizada para la toma de decisiones.

Comentario: Esta política logra un descubrimiento completo acerca de la naturaleza de la información utilizada para la toma de decisiones. La gerencia debe saber hasta qué punto puede confiar en la información que recibe. Esta información acerca de la integridad ayuda a la gerencia en la toma de decisiones acerca de si la información es confiable y cuán factible será que las decisiones que tomó sean precisas. Puede desarrollarse un texto explicativo que acompañe a esta política. Este texto puede dar formas específicas de medir la integridad informática. Por ejemplo, puede indicarse el

lapso de tiempo que transcurre entre la obtención de los datos y la presentación de la información procesada. El análisis de los atributos de integridad de la información es efectuado por los administradores de las bases de datos, modeladores de datos, arquitectos de sistemas y demás personal que trabaja en la normalización de los datos en base a aplicaciones y plataformas cruzadas. Los especialistas de seguridad informática pueden estar involucrados, a pesar de que este trabajo generalmente no forma parte de sus funciones.

Políticas Relacionadas: “[Naturaleza y Ubicación de la Información de la Organización](#)” e “[Información Incompleta u Obsoleta](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Revisión de los Controles de los Sistemas Informáticos — Interno

Política: El Auditor Interno debe revisar periódicamente lo adecuado de los controles respecto de los sistemas informáticos y el cumplimiento de dichos controles.

Comentario: Esta política establece las responsabilidades del Auditor Interno relacionadas con la seguridad informática. En algunas organizaciones, el Auditor Interno no tiene la suficiente experiencia para realizar este trabajo, así que ignora la seguridad informática. Esta política notifica al Auditor Interno que debe ser entrenado de forma que pueda llevar a cabo esta tarea, contrate un auditor de tecnología de la información o mantenga a un consultor externo que lo pueda asistir en este trabajo. En lugar del Auditor Interno, la gerencia de Seguridad Informática puede llevar a cabo estas revisiones de seguridad. El objetivo importante es asignar claramente la responsabilidad. La política puede ser modificada para reflejar el hecho de que a menudo el Auditor Interno verifica la suficiencia de la seguridad informática en lugar de llevar a cabo el trabajo técnico específico.

Políticas Relacionadas: “[Registros de Auditoría en los Sistemas](#)” y “[Evaluación del Riesgo en los Sistemas de Producción](#)”

Política Dirigida a: Gerencia

12.03.02 Protección de los Rastros de Auditoría de Sistemas

1. Código Fuente del Software de Penetración de Sistemas

Política: El código fuente de programación y sus respectivos análisis técnicos usados para garantizar la seguridad, debe ser divulgado únicamente a aquellas personas que tengan una necesidad demostrable de conocerlos.

Comentario: Esta política evita que personas no autorizadas utilicen esta información para comprometer los sistemas de seguridad. Muchos criminales de computación utilizan material previamente escrito para lograr nuevos objetivos. Por ejemplo, muchos de los virus que infectan a los sistemas son simples derivados de virus antiguos. El análisis de estas rutinas de penetración en el sistema es también sensible debido a

Ambientes de Seguridad: Todos

3. Verificación de Cumplimiento de Seguridad Informática

Política: El Auditor Interno debe llevar a cabo la verificación del cumplimiento de las políticas, normas y procedimientos relacionados con la seguridad informática.

Comentario: Esta política establece que el Auditor Interno y no la gerencia de Seguridad Informática debe llevar a cabo la verificación de conformidad. Si la gerencia de Seguridad Informática lo hiciera, se presentaría un conflicto de intereses. No es deseable que las personas que diseñan, instalan y administran un sistema también lo auditén. Mientras que la gerencia de Seguridad Informática puede instalar y ejecutar herramientas que ayuden a reforzar estas políticas, normas y procedimientos, la responsabilidad de la verificación de conformidad debe ser asignada al Auditor Interno.

Políticas Relacionadas: “[Revisión de los Controles de los Sistemas Informáticos — Interno](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

que puede ser utilizado por los atacantes de sistemas para conocer acerca de aquello que funciona y aquello que no. Este análisis puede ser considerado como una lista de mejoras necesarias en el sistema para una nueva generación de software para ataques al sistema. También es preocupante la susceptibilidad de la organización de desplegar información sensible sobre vulnerabilidades.

Políticas Relacionadas: “[Divulgación de las Vulnerabilidades del Sistema Informático](#),” “[Comprometer Mecanismos de Seguridad para los Clientes](#),” y “[Presentación de la Imagen Pública](#)”

Política Dirigida a: Gerencia y personal técnico

Ambientes de Seguridad: Todos

2. Identificación de Vulnerabilidades

Política: Todos los sistemas conectados directamente a Internet deben estar sujetos a una verificación automática de riesgo, llevada a cabo a través de software para identificación de vulnerabilidades por lo menos una vez al mes.

Comentario: El objetivo de esta política es asegurar que la Empresa X conozca cuáles vulnerabilidades puede aprovechar un hacker para invadir sus sistemas. Con esta información, el personal de la Empresa X puede hacer los ajustes adecuados, como por ejemplo instalar la última versión de determinados programas de sistemas. Si el personal desconoce sus vulnerabilidades, será imposible que lleve a cabo los ajustes necesarios.

Esta política sustenta la conclusión a la que han llegado varios estudios estadísticos de que es menos costoso prevenir o recuperarse de problemas que corregirlos. El software para identificación de vulnerabilidades es especialmente importante para sistemas conectados a Internet debido a que estos sistemas están expuestos a ataques mucho más severos que otros sistemas.

Políticas Relacionadas: ‘‘Sistemas de Detección de Intrusos,’’ ‘‘Contraseñas Proporcionadas por Proveedores,’’ y ‘‘Evidencia de Delito o Abuso Informático’’

Política Dirigida a: Personal técnico

Ambientes de Seguridad: Todos



Capítulo 4 MODELO DE POLÍTICA DE SEGURIDAD INFORMÁTICA DE ALTO NIVEL

Rol de la Información y los Sistemas Informáticos—La Empresa X depende en forma crítica de la información y de los sistemas informáticos. Si se revela información importante a personas inapropiadas, la empresa puede sufrir pérdidas considerables o salir del negocio. La buena reputación de la Empresa X está directamente relacionada con la manera en que maneja tanto la información como los sistemas informáticos. Por ejemplo, si se hace pública información confidencial de un cliente, la reputación de la empresa se vería afectada. Por ésta y otras importantes razones de negocio, la gerencia ejecutiva en conjunto con la junta directiva ha iniciado y continúa manteniendo un esfuerzo de seguridad informática. Parte de este esfuerzo es la definición de estas políticas de seguridad informática.

Esfuerzo de Equipo—Para que sea efectiva, la seguridad informática debe constituir un esfuerzo que involucre la participación y soporte de todos los empleados de la Empresa X que tengan que ver con la información y los sistemas informáticos. Al reconocer la necesidad de un equipo de trabajo, esta declaración establece las responsabilidades de los usuarios y los pasos que deben seguir a fin de ayudar a proteger la información y los sistemas informáticos de la Empresa X. Este documento describe las maneras de prevenir y reaccionar ante una variedad de amenazas en contra de la información y de los sistemas informáticos, tales como el acceso no autorizado, la divulgación, la duplicación, la modificación, el apropiamiento, la destrucción, la pérdida, la mala utilización y la negativa de uso.

Personas Involucradas—Todo empleado de la Empresa X debe cumplir las políticas de seguridad informática que se encuentran en éste y en otros documentos correspondientes. Los empleados que deliberadamente violen ésta y otras declaraciones sobre políticas de seguridad informática estarán sujetos a acciones disciplinarias que pueden incluir el cese de sus funciones.

Sistemas Involucrados—Esta política se aplica a todos los computadores y sistemas en red que posea o sean administrados por la Empresa X. Esta política se aplica a todos los sistemas operativos, tamaños de computadores y aplicaciones. La política abarca solamente la

información manejada por computadores y redes. A pesar de que este documento hace mención a otras presentaciones de información como la voz o el papel, no enfatiza directamente estas formas de seguridad informática. Para obtener información acerca de la protección de la información en papel, ver la Política de Clasificación de la Información [puede insertarse aquí un enlace a una página en Intranet para ese documento].

Principales Departamentos que Trabajan en Seguridad Informática—El departamento de Seguridad Informática es el que centraliza, dirige y autoriza las actividades de seguridad informática de todas las unidades organizacionales de la Empresa X [inserte el enlace de Intranet a la misión de Seguridad Informática]. La Seguridad Informática es responsable de establecer y mantener a lo largo de toda la organización, las políticas de seguridad informática, las normas, los lineamientos y los procedimientos. La unidad de Auditoría de Tecnología Informática que forma parte del departamento de Auditoría Interna es la responsable de verificar y garantizar que todas las unidades organizativas están operando en forma consistente con estos requerimientos [inserte un enlace a la misión de Auditoría Interna]. La investigación sobre intrusiones en el sistema y otros incidentes de seguridad informática son responsabilidad del departamento de Seguridad Física [inserte un enlace de Intranet a la misión de Seguridad Industrial]. Las materias disciplinarias resultantes de violaciones a los requerimientos de seguridad informática son manejadas por los gerentes locales que trabajan conjuntamente con el departamento de Recursos Humanos [inserte un enlace de Intranet a la misión del departamento de Recursos Humanos].

Tres Categorías de Responsabilidad—Para coordinar un esfuerzo de equipo, la Empresa X ha establecido tres categorías, y al menos una de ellas se aplica a todo empleado. Estas categorías son: Propietario, Custodio y Usuario. Estas categorías definen las responsabilidades generales con respecto a la seguridad informática. Puede encontrarse información más detallada sobre estas responsabilidades en la Política de Propiedad de la Información [inserte un enlace a ese documento].

Responsabilidades del Propietario—Los Propietarios de la Información son los gerentes de departamento, los integrantes de la alta gerencia o sus delegados dentro de

la Empresa X, que asumen la responsabilidad de la adquisición, desarrollo y mantenimiento de las aplicaciones de producción que procesan la información de la Empresa X. Las aplicaciones de producción son programas computarizados que regularmente proveen informes que soportan la toma de decisiones y otras actividades de negocios. Toda la información sobre los sistemas de aplicaciones de producción debe tener un Propietario designado. Para cada tipo de información, los Propietarios indican la clasificación del grado de confidencialidad, determinan el nivel apropiado de criticidad, definen cuáles usuarios recibirán el acceso y autorizan las peticiones sobre las distintas maneras de utilizar la información.

Responsabilidades del Custodio—Los Custodios tienen la posesión física o lógica de la información de la Empresa X o de aquélla que ha sido confiada a la Empresa X. Si bien los integrantes del equipo del departamento de Tecnología Informática son claramente Custodios, también lo son los administradores del sistema local. Cuando la información se mantiene solamente en un computador personal, el Usuario también es un Custodio. Cada clase de información contenida en los sistemas de aplicaciones de producción información debe tener uno más Custodios designados. Los Custodios son responsables de salvaguardar la información, incluyendo la implementación de sistemas de control de acceso para evitar la divulgación inadecuada y hacer respaldos de forma que no se pierda información crítica. Los Custodios también deben implementar, operar y mantener las medidas de seguridad definidas por los Propietarios de la información.

Responsabilidades del Usuario—Los Usuarios son responsables de conocer y cumplir todas las políticas, procedimientos y normas relativos a la seguridad informática de la Empresa X. Las preguntas acerca del manejo adecuado de un tipo específico de información deben ser dirigidas directamente al Custodio o al Propietario de dicha información.

Manejo Consistente de la Información—La información de la Empresa X, o aquélla que le ha sido confiada, debe ser protegida de manera proporcional a su nivel de confidencialidad y criticidad. Deben emplearse medidas de seguridad sin importar el medio en que ha sido almacenada la información, los sistemas que la procesan o los métodos a través de los cuales es transportada. La información debe ser protegida en forma consistente con su clasificación, sin importar en qué fase de su ciclo de vida se encuentre, desde el origen hasta la destrucción.

Designaciones para la Clasificación de la Información—La Empresa X ha adoptado un sistema para clasificar la información, dividiéndola en cuatro grupos. Toda la información bajo el control de la Empresa X, sea generada interna o externamente, se encuentra en alguna de estas categorías: Secreta, Confidencial, Uso Interno Solamente o Pública. Todos los empleados deben familiarizarse con las definiciones de estas categorías y con los pasos a seguir para proteger la información que corresponde a estas categorías. Pueden encontrarse detalles al respecto en la Política de Clasificación de la Información [inserte un enlace aquí]. Para los efectos de esta política, "información sensible" es la información que se encuentra en la categoría de Secreta o Confidencial.

Etiquetado de la Clasificación de la Información—Si la información es sensible, desde el momento en que es creada hasta el momento en que es destruida o desclasificada, debe ser etiquetada con una designación apropiada de clasificación de información. Este tipo de marcas deben aparecer en todas las manifestaciones de la información. La gran mayoría de la información de la Empresa X corresponde a la categoría de Uso Interno Solamente. Por esta razón, no es necesario etiquetarla. La información que no es etiquetada por descarte se clasifica como Uso Interno Solamente. Puede encontrarse información adicional acerca del etiquetado de información sensible en la Política de Clasificación de la Información [inserte un enlace aquí].

Necesidad de Conocer—El acceso a información en posesión o bajo el control de la Empresa X debe proporcionarse de acuerdo al concepto de la necesidad de conocer. La información debe ser divulgada únicamente a aquellas personas que tienen una necesidad legítima que se deriva de asuntos de negocios. Al mismo tiempo, los empleados no pueden negar el acceso a información cuando el Propietario exige u ordena que sea compartida. Para implementar el concepto de necesidad de conocer, la Empresa X ha adoptado un proceso de solicitud de acceso y autorización por parte del Propietario. Los empleados no deben intentar acceder a información sensible a menos que el Propietario les haya dado el derecho al acceso. Cuando un empleado cambia sus responsabilidades, incluyendo cese laboral, transferencia, promoción y permiso remunerado, su supervisor debe notificar inmediatamente al departamento de Seguridad Informática [inserte un enlace a otra pantalla que muestre los detalles de este proceso de notificación]. Los privilegios que se otorgan a todos los empleados deben ser revisados periódicamente por los

Propietarios y Custodios para garantizar que únicamente aquéllos con necesidad actual de conocimiento tengan acceso a la información.

identificadores de Usuario y Contraseñas—Para implementar el proceso de necesidad de conocer, la Empresa X requiere que cada empleado que accede a sistemas informáticos multiusuario tenga un único identificador y una contraseña. Estos identificadores de usuario deben ser empleados para restringir los privilegios informáticos con base en las responsabilidades del trabajo, del proyecto y de otras actividades de negocios. Cada empleado es responsable por el uso de su identificador y contraseña.

Identificadores de Usuarios Anónimos—Con excepción de los boletines electrónicos, sitios de Internet, sitios de Intranet y otros sistemas en los que los usuarios regulares permanecen anónimos, los usuarios tienen prohibido conectarse a cualquier sistema o red de la Empresa X en forma anónima. El acceso anónimo podría, por ejemplo, involucrar el uso de identificadores de usuarios "invitados". Cuando los usuarios emplean comandos del sistema que les permiten cambiar identificadores de usuarios activos para obtener ciertos privilegios, deben haberse conectado inicialmente empleando identificadores de usuarios que claramente indican sus identidades.

Contraseñas Difíciles de Adivinar—Los usuarios deben escoger contraseñas que sean difíciles de adivinar. Esto significa que las contraseñas no pueden estar relacionadas con su trabajo o con su vida privada. Por ejemplo, no pueden utilizarse el número de placa del automóvil, el nombre del cónyuge o partes de una dirección. Esto también significa que las contraseñas no pueden ser una palabra de las que se encuentran en diccionarios o cualquier parte gramatical. Por ejemplo, no deben usarse nombres propios, lugares, términos técnicos o expresiones comunes.

Contraseñas Fáciles de Recordar—Los usuarios pueden escoger contraseñas fáciles de recordar que al mismo tiempo sean difíciles de adivinar por terceros no autorizados si:

- Reúnen varias palabras en una sola.
- Mueven una palabra una fila hacia arriba, abajo, izquierda o derecha en el teclado.
- Mueven los caracteres de una palabra un número determinado de letras hacia arriba o abajo en el alfabeto.

- Transforman una palabra de acuerdo con un método específico, como convertir una letra en un número que refleja su posición dentro de la palabra.
- Combinan puntuación o números en una palabra.
- Forman acrónimos de palabras de canciones, poemas u otra secuencia conocida de palabras.
- Escriben mal una palabra deliberadamente.
- Combinan algunas preferencias como el horario preferido de acostarse y los colores favoritos.

Patrones Repetitivos en Contraseñas—Los usuarios no deben construir contraseñas usando una secuencia básica de caracteres que cambia parcialmente en función de la fecha o de otro factor predecible. Los usuarios no deben construir contraseñas que son idénticas o sustancialmente similares a contraseñas que hayan utilizado con anterioridad.

Restricciones de las Contraseñas—Las contraseñas deben tener al menos 10 caracteres de longitud. Deben ser cambiadas cada 90 días o a intervalos más frecuentes. Cuando un empleado sospecha que su contraseña la conoce otra persona, debe cambiarla inmediatamente.

Almacenamiento de las Contraseñas—Las contraseñas no deben almacenarse en forma legible en archivos por lotes, comandos para acceso automático, macros de software, teclas de función, en computadores que no posean sistemas de control de acceso o en cualquier otra ubicación en donde personas no autorizadas puedan descubrirlas. Tampoco pueden escribirse en una forma fácilmente descifrable y dejarse en un lugar en el que puedan ser descubiertas por personas no autorizadas.

Compartir Contraseñas—Si los empleados necesitan compartir información residente en el computador, deben utilizar el correo electrónico, las bases de datos grupales, directorios en los servidores de la red de área local, intercambio manual con discuetes y otros mecanismos. A pesar de que los identificadores de usuario se comparten en el correo electrónico y con otros fines, las contraseñas nunca deben compartirse ni revelarse a otros. Los administradores del sistema y el equipo técnico de sistemas informáticos nunca deben pedirle a un empleado que revele su contraseña. Únicamente cuando se crea la contraseña podría ser conocida por otro. Estas contraseñas temporales deben ser cambiadas la primera vez que el usuario autorizado accede al sistema. Si el usuario sospecha que su identifi-

cador de usuario y contraseña han sido utilizados por alguien más, debe notificarlo inmediatamente al administrador del sistema informático.

Declaración de Conformidad—Todos los empleados que deseen utilizar los sistemas de computadores multiusuario de la Empresa X deben firmar una declaración de conformidad antes de que se les otorgue el identificador de usuario [inserte un enlace a la declaración]. Cuando ya poseen identificadores de usuario, deben firmar la declaración antes de recibir la renovación anual de sus identificadores de usuario. La firma de la declaración de conformidad indica que el usuario involucrado comprende y conviene en adherirse a las políticas y procedimientos de la Empresa X relacionados con los computadores y redes, incluyendo las instrucciones contenidas en esta política.

Divulgación de Información a Terceros—A menos que haya sido específicamente designada como pública, toda la información interna de la Empresa X debe ser protegida contra su divulgación a terceros. Pueden recibir acceso a esta información únicamente si existe y es demostrable la necesidad de conocer, cuando se ha firmado un acuerdo de sensibleiedad [inserte un enlace a una copia del acuerdo] y cuando esta divulgación ha sido expresamente autorizada por el Propietario relevante de la información de la Empresa X [inserte un enlace al diccionario de datos corporativos con una lista de los Propietarios y los tipos de información que manejan]. Si se pierde o se sospecha de la pérdida o divulgación a terceros no autorizados de información sensible, el Propietario de la información y el departamento de Seguridad Informática deben ser notificados inmediatamente [inserte un enlace a una pantalla independiente con los números telefónicos e instrucciones adicionales para este proceso de notificación].

Solicitud de Terceros de Información de la Empresa X—A menos que el empleado haya sido autorizado por el Propietario de la información para divulgarla públicamente, todas las solicitudes de información acerca de la Empresa X y su negocio deben ser dirigidas al departamento de Relaciones Públicas. Estas solicitudes incluyen cuestionarios, investigaciones y entrevistas por la prensa. Esta política no se aplica a la información de ventas y mercadeo de los productos y servicios de la Empresa X ni se refiere a las llamadas de soporte técnico de los clientes. Si un empleado recibe información sensible desde terceros en beneficio de la Empresa X, esta recepción debe estar precedida de la firma de este tercero de un formulario de liberación de la Empresa X [inserte un enlace al formulario]. Para obtener más detalles acerca de este tópico, consulte la

Política de Divulgación de Información de parte de Terceros [inserte un enlace]. Puede encontrarse información adicional relevante en la Política de Seguridad de Comunicaciones Externas [inserte un enlace].

Seguridad Física para Controlar el Acceso a la Información—Debe restringirse el acceso físico a cualquier oficina, sala de computadores u otra área de trabajo de la Empresa X que contenga información sensible. Cuando no es utilizada, la información sensible siempre debe estar protegida contra la divulgación no autorizada. La información sensible en papel debe guardarse bajo llave en contenedores apropiados cuando se deja en una oficina sin vigilancia. Si el Custodio de este tipo de información considera que estará fuera por menos de 30 minutos, la información en papel puede dejarse sobre el escritorio o en cualquier otro lugar visible sólo si todas las puertas y ventanas de la oficina se encuentran cerradas bajo llave. Fuera del horario de trabajo, los empleados que trabajan en áreas que contienen información sensible deben guardar bajo llave toda la información. A menos que la información esté siendo utilizada por personal autorizado, los escritorios deben mantenerse limpios y sin documentos fuera del horario de trabajo para evitar el acceso no autorizado a la información. Los empleados deben colocar las pantallas de sus computadores en una posición en la que se evite que personal no autorizado pueda ver la información sensible que se encuentre desplegada en ellas.

Conexiones Internas de Red—Todos los computadores de la Empresa X que almacenan información sensible y que están permanente o intermitentemente conectados a las redes internas deben tener un sistema de control de acceso mediante contraseñas aprobado por el departamento de Seguridad Informática. Al margen de las conexiones de red, todos los computadores no conectados que manejan información sensible también deben tener un sistema aprobado de control de acceso con contraseñas [inserte un enlace a la lista de productos autorizados de seguridad informática y los detalles sobre cómo ordenarlos]. Los usuarios que trabajan con otras clases de computadores deben emplear las contraseñas del protector de pantalla provistas por los sistemas operativos, de forma tal que después de un período de inactividad, la información en pantalla desaparezca hasta que se introduzca la contraseña apropiada. Los sistemas multiusuario a lo largo de la Empresa X deben emplear sistemas de desconexión automática que finalizan la sesión del usuario después de un determinado período de inactividad.

Conexiones Externas de Red—Todas las sesiones entrantes de conexión a los computadores de la Empresa X desde redes externas deben estar protegidas con un sistema autorizado de control de acceso mediante contraseñas dinámicas [inserte un enlace a la lista de productos aprobados de seguridad informática]. Las contraseñas dinámicas son diferentes cada vez que se usan, por lo que no pueden ser reutilizadas para obtener acceso no autorizado. Los usuarios con computadores personales conectados a redes externas tienen prohibido dejar conectados sin supervisión los módems mientras funcione el software de comunicación de datos, a menos que previamente se haya instalado un sistema autorizado de contraseñas dinámicas. Cuando usen los computadores de la Empresa X, los empleados no pueden establecer conexiones con redes externas, incluyendo proveedores de servicios de Internet, a menos que estas conexiones hayan sido autorizadas por el departamento de Seguridad Informática. Para obtener más información acerca de este proceso, vea la Política de Seguridad de Comunicaciones Externas [inserte un enlace].

Modificaciones a las Redes—Con excepción de situaciones de emergencia, todos los cambios en las redes computarizadas de la Empresa X deben estar documentados en una orden de trabajo y autorizados previamente por el departamento de Tecnología Informática. Todos los cambios de emergencia a las redes de la Empresa X deben ser efectuados únicamente por personas autorizadas por el departamento de Tecnología Informática. Este proceso evita cambios inesperados que puedan conducir a la negación de algún servicio, divulgación no autorizada de información y otros problemas. Este proceso se aplica no solamente a los empleados sino también al personal de ventas.

Teletrabajo—A discreción de la gerencia, cierto personal calificado puede llevar trabajo a su casa. Este permiso debe ser otorgado por el supervisor inmediato de cada empleado en función de un listado de verificación de factores relevantes [inserte un enlace al listado de verificación, que podría ser una página en Intranet dentro de la página principal del departamento de Recursos Humanos en Intranet]. El permiso permanente de llevar trabajo a casa depende parcialmente de la continua conformidad con ciertas políticas de seguridad informática y normas. Para obtener más información sobre estos requisitos, vea la Política de Teletrabajo [inserte un enlace]. El chequeo periódico del correo electrónico en la vía desde o hacia la casa no se considera como llevar trabajo a casa, sin embargo, requiere que los empleados tomen las mismas precauciones de seguridad.

Acceso a Internet—Los empleados están provistos de acceso a Internet para llevar a cabo sus tareas, pero este acceso puede darse por terminado en cualquier momento a discreción del supervisor inmediato del empleado. El acceso a Internet es monitoreado para asegurar que los empleados no visiten sitios no relacionados con su trabajo y también para garantizar el cumplimiento de las políticas de seguridad. Los empleados deben tener especial cuidado en no representar a la Empresa X en grupos de discusión por Internet o en otros foros públicos, a menos que hayan recibido previamente autorización de la alta gerencia para así hacerlo. Toda la información que se recibe de Internet debe ser considerada sospechosa hasta que se confirme con fuentes confiables. Los empleados no deben colocar material de la Empresa X en sistemas de computación accesibles públicamente como por ejemplo Internet, a menos que haya sido aprobado tanto por el Propietario de la información como por el departamento de Tecnología Informática. La creación de páginas en Internet es manejada en forma independiente mediante un proceso de aprobación que involucra al comité de comunicaciones externas [inserte un enlace al departamento de Relaciones Públicas]. Los usuarios tienen prohibido efectuar transacciones de comercio electrónico por Internet a menos que los departamentos de Tecnología Informática y Seguridad Informática hayan aprobado este tipo de actividades. La información sensible, incluyendo contraseñas y números de tarjetas de crédito, no debe ser enviada a través de Internet a menos que se encuentre cifrada. Estas y otras consideraciones se discuten en mayor detalle en la Política de Comunicaciones en Internet [inserte un enlace].

Correo Electrónico—Todo trabajador de la Empresa X que utiliza computadores recibirá una dirección de correo electrónico con sus privilegios correspondientes. En todas las comunicaciones de la Empresa X, que envíe o reciba por correo electrónico, debe utilizar esta dirección de correo electrónico de la compañía. No puede utilizar para actividades de negocios de la Empresa X una dirección electrónica de correo personal de un proveedor de servicios de Internet a menos que reciba la autorización de la gerencia. Cuando los trabajadores transmitan mensajes a grupos de personas fuera de la Empresa X, deben utilizar copias de carbón o listas de distribución. Están prohibidas las transmisiones por correo electrónico no solicitadas a clientes o prospectos. También está prohibido enviar mensajes emotivos y sobrecargar la cuenta de correo electrónico con grandes cantidades de mensajes. Todas las comunicaciones de trabajo transmitidas por correo electrónico deben ser revisadas antes de enviarse y tener una apariencia y tono profesional y de negocios. El correo

electrónico es un método de comunicación público muy parecido a una postal. Todos los trabajadores de la Empresa X deben abstenerse de enviar números de tarjetas de crédito, contraseñas o cualquier otra información confidencial que pueda ser interceptada. Todo el personal de la Empresa X debe emplear una firma normalizada de correo electrónico que incluya su nombre completo, cargo, dirección de trabajo y número telefónico del trabajo. Los usuarios no deben almacenar mensajes importantes en la bandeja de entrada. Pueden encontrarse detalles adicionales en la Política de Seguridad del Correo Electrónico [inserte un enlace].

Software antivirus—Todos los usuarios de computadores personales deben tener versiones actualizadas de software antivirus ejecutándose en sus computadores [inserte un enlace a la lista de productos autorizados de seguridad informática]. Los usuarios no deben abortar procesos automáticos de actualización de antivirus. El software antivirus debe utilizarse para revisar todos los archivos y programas provenientes de terceros o de otros grupos de la Empresa X. Esta revisión debe hacerse antes de abrir nuevos archivos de datos o de ejecutar nuevos programas. Los trabajadores no deben dejar de utilizar o desactivar el proceso de revisión que podría evitar la transmisión de un virus.

Eradicación de Virus—Si los trabajadores sospechan que el computador está infectado con un virus, deben dejar de utilizarlo inmediatamente y llamar al Centro de Atención al Usuario [inserte un enlace a la página de asistencia técnica]. No deben intercambiarse disquetes ni otros medios de almacenamiento magnético entre el computador infectado y otros computadores hasta que el virus haya sido exitosamente erradicado. El computador infectado debe ser inmediatamente aislado de las redes internas. Los usuarios no deben intentar erradicar los virus por sí mismos. El personal calificado de la Empresa X o consultores deben llevar a cabo esta tarea de manera que se minimicen tanto la destrucción de los datos como el tiempo de caída del sistema.

Respaldos Limpios—Todos los programas de los computadores personales deben ser copiados antes de ser utilizados por primera vez y estas copias deben almacenarse en lugares seguros, como un gabinete bajo llave. Estas copias maestras no deben ser utilizadas en las actividades cotidianas del negocio sino ser guardadas, en caso de recuperación por infecciones de virus, fallas del disco duro y otros problemas.

Fuentes de Software—Los computadores y redes de la Empresa X no deben ejecutar programas que provengan de fuentes distintas de los departamentos de la Empresa X, los usuarios conocidos y confiables, las autoridades

reconocidas de sistemas de seguridad, o los proveedores establecidos de computadores, redes o software. No deben utilizarse los programas que se descargan de boletines electrónicos, dominios públicos y otras fuentes no confiables a menos que hayan sido objeto de rigurosas pruebas aprobadas por el departamento de Seguridad Informática [inserte un enlace a la página que describe este proceso y a quién contactar].

Especificaciones Escritas para los Propietarios—Todos los programas desarrollados internamente, para procesar información crítica o sensible de la Empresa X, deben tener una especificación formal por escrito. Esta especificación debe incluir una discusión sobre riesgos de seguridad y controles como sistemas de control de acceso y planes de contingencia. La especificación debe formar parte de un acuerdo entre el Propietario de la información y el desarrollador del sistema. En este caso no se consideran programas las macros para hojas de cálculo y los documentos elaborados en procesadores de palabras.

Requisito de Autorización por Seguridad—Antes de utilizar aplicaciones nuevas o sustancialmente modificadas en el procesamiento de producción, debe existir una autorización escrita del departamento de Seguridad Informática con relación a los controles que deben emplearse. Este requisito se aplica tanto a computadores personales como a sistemas más grandes [inserte un enlace a una planilla solicitando la revisión y aprobación del departamento de Seguridad Informática].

Control Formal de Cambios—Todos los computadores y sistemas de comunicación utilizados para el procesamiento de producción deben emplear un proceso documentado de control de cambios, de forma tal que se garantice que solamente se realicen cambios autorizados. Este procedimiento de control de cambios debe utilizarse para todos los cambios significativos en los sistemas de producción, hardware, enlaces de comunicación y procedimientos. Esta política se aplica a los computadores personales en donde se ejecutan sistemas de producción y en grandes sistemas multiusuario. Para obtener más información acerca de este tema, vea la Política de Desarrollo de Software y Control de Cambios [inserte un enlace].

Convenciones para Desarrollo de Sistemas—Todas las actividades de desarrollo de software de producción y de mantenimiento llevadas a cabo internamente deben cumplir las políticas, normas y procedimientos del departamento de Tecnología Informática y demás convenciones de desarrollo de sistemas. Estas convenciones incluyen la correcta verificación, adiestramiento

y documentación. Para obtener más información acerca de este tópico vea la Política de Desarrollo de Software y Control de Cambios [inserte un enlace].

Licencias Adecuadas—La gerencia de la Empresa X debe hacer arreglos adecuados con los proveedores de software para obtener copias adicionales con licencia en caso de que éstas sean necesarias para actividades de negocios. Todos los programas deben ser adquiridos a través del departamento de Compras [inserte un enlace a la lista de programas de computación autorizados y un enlace a la planilla para solicitud de compra del departamento de Compras].

Copias No Autorizadas—Los usuarios no deben copiar los programas suministrados por la Empresa X en ningún medio de almacenamiento, transferir dichos programas a otro computador ni hacerlos públicos a terceros sin el permiso previo de su supervisor. Las copias de respaldo son una excepción autorizada de esta política.

Responsabilidad de Respaldar—Los usuarios de computadores personales deben respaldar con regularidad la información almacenada en sus computadores o asegurarse de que alguien lo haga por ellos. En el caso de computadores multiusuario y sistemas de comunicación, el administrador del sistema es responsable de realizar respaldos periódicos. Si es solicitado, el departamento de Tecnología Informática debe instalar o proveer asistencia técnica para la instalación de dispositivos de hardware y software para respaldos [inserte un enlace a la lista de productos de seguridad autorizados]. Todos los respaldos que contengan información crítica o confidencial deben ser almacenados en una ubicación aprobada fuera del sitio de respaldo, en donde existan controles de acceso físico o cifrado. Debe prepararse un plan de contingencia para todas las aplicaciones que manejan información crítica de producción. Es responsabilidad del Propietario de la información garantizar que este plan se desarrolle adecuadamente, que se actualice regularmente y que se pruebe periódicamente.

Protección Antirrobo—Todos los computadores y redes de la Empresa X deben estar físicamente asegurados con dispositivos antirrobo en caso de que se encuentren en una oficina de libre acceso. Los servidores de redes locales y otros sistemas multiusuario deben colocarse en gabinetes, armarios o salones de computación bajo llave. Los computadores portátiles que se encuentren en una oficina de libre acceso y que no se estén usando también deben estar asegurados con cables bloqueadores, colocados en gabinetes cerrados o asegurados con cualquier otro sistema de bloqueo. Los equipos de redes y computación no pueden ser

removidos de las oficinas de la Empresa X, a menos que la persona que quiera hacerlo haya obtenido la autorización de la gerencia del edificio. Los celulares y beepers no están sujetos a estos requisitos.

Divulgación de la Información de Seguridad—La información acerca de las medidas de seguridad para los computadores y sistemas de red de la Empresa X es confidencial y no debe ser divulgada a personas que no sean usuarios autorizados de dichos sistemas a menos que lo autorice el director de Seguridad Informática. Por ejemplo, está prohibido publicar en directorios los números telefónicos del módem u otra información de acceso a los sistemas. Se permite la publicación de direcciones de correo electrónico.

Derechos sobre el Material Desarrollado—Mientras los trabajadores desempeñen labores para la Empresa X, deben ceder a ésta los derechos exclusivos sobre patentes, derechos de autor, de invenciones o de propiedad intelectual de todo lo que creen o desarrollen. Todos los programas y documentación generados o provistos por los trabajadores para beneficio de la Empresa X son propiedad de la Empresa X. La Empresa X tiene la propiedad sobre los contenidos de todos los sistemas informáticos bajo su control. La Empresa X se reserva el derecho de acceder y utilizar esta información a su discreción.

Derecho a Investigar y Monitorear—La gerencia de la Empresa X se reserva el derecho de monitorear, inspeccionar o investigar en cualquier momento todos sus sistemas informáticos. Este examen puede hacerse con o sin el consentimiento, presencia o conocimiento de los trabajadores correspondientes. Los sistemas informáticos que estén sujetos a este tipo de examen incluyen, pero no se limitan a los archivos del sistema de correo electrónico, archivos en el disco duro del computador personal, archivos de correo de voz, archivos a imprimir, documentos recibidos de la máquina de fax, las gavetas de los escritorios y las áreas de almacenamiento. Todas las búsquedas de esta naturaleza deben llevarse a cabo después de obtener la autorización de los departamentos Legal y de Seguridad Informática. Debido a que los computadores y redes de la Empresa X son proporcionados únicamente con fines de negocios, los trabajadores no deben esperar que exista privacidad en la información que almacenen o envíen a través de estos sistemas informáticos. La gerencia de la Empresa X tiene el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal. Para obtener más información acerca de este tópico, consulte la Política de Privacidad de la Información [inserte un enlace].

Uso Personal—Los sistemas informáticos de la Empresa X deben ser utilizados únicamente con fines de negocios. El uso personal en forma incidental es permisible si no consume más que un número trivial de recursos que podrían de otra manera ser utilizados con propósitos de negocios, si no interfiere con la productividad del trabajador y no está en contra de cualquier actividad de negocios. El uso incidental permisible del sistema de correo electrónico podría involucrar, por ejemplo, el envío de un mensaje para planificar un almuerzo. El uso personal que no se encuentre en estas tres categorías debe ser autorizado previamente por el gerente del departamento. Los juegos computarizados que se encuentren en los sistemas operativos pueden usarse durante los recesos o la hora de almuerzo, siempre que esta actividad no interfiera con la productividad del trabajador. Se prohíbe el uso de juegos que se encuentren en paquetes de software independientes. Está prohibido el uso de los sistemas informáticos de la Empresa X para enviar cadenas de cartas, peticiones de caridad, material de campañas políticas, trabajo religioso, para la transmisión de material objetable o cualquier otro uso con fines no relacionados con el negocio.

Conducta Inapropiada—La gerencia de la Empresa X se reserva el derecho de revocar los privilegios informáticos a cualquier usuario en cualquier momento. No es permisible la conducta que interfiera con la normal y adecuada operación de los sistemas informáticos de la Empresa X que adversamente afecte la capacidad de otros de utilizar estos sistemas informáticos o que sea dañina u ofensiva para otros.

Herramientas que Comprometen la Seguridad—A menos que hayan sido expresamente autorizados por el departamento de Seguridad Informática, los trabajadores de la Empresa X no pueden adquirir, poseer, comerciar o utilizar herramientas de hardware o

software que puedan ser empleadas para evaluar o comprometer la seguridad de los sistemas informáticos. Pueden ser ejemplos de estas herramientas aquéllas que frustran la protección de copiado de programas, descubren contraseñas secretas, identifican vulnerabilidades en la seguridad o descifran archivos cifrados. Sin esta clase de autorización, los trabajadores tienen prohibido utilizar cualquier clase de hardware o software que monitoree el tráfico en una red o las actividades de un computador.

Actividades Prohibidas—Los usuarios no deben examinar o intentar comprometer las medidas de seguridad de los computadores o sistemas de comunicación, a menos que hayan sido previamente autorizados por escrito por el director del departamento de Auditoría Interna. Los incidentes que involucren actividades no autorizadas en el sistema, adivinado de contraseñas, descifrado de archivos, contrabando de copias de software, o cualquier otro intento similar de comprometer las medidas de seguridad, pueden ser ilegales y serán considerados como una seria violación de la política interna de la Empresa X. Están absolutamente prohibidos los atajos que circundan las medidas de seguridad, las travesuras y bromas prácticas que comprometan las medidas de seguridad de los sistemas.

Informes Obligatorios—Todas las violaciones de políticas de las que se tenga sospecha, intrusiones en el sistema, contaminaciones por virus o cualquier otra condición que pueda amenazar la información o los sistemas informáticos de la Empresa X, deben ser inmediatamente informadas al departamento de Seguridad Informática [correo de voz con el alerta XXX-XXX-XXXX] [inserte un enlace a la página web en Intranet al equipo de respuesta ante emergencias computacionales]. Los mensajes dejados en este buzón de correo de voz pueden ser anónimos.



Capítulo 5

MODELO DE POLÍTICA DE SEGURIDAD INFORMÁTICA DETALLADA

Resumen Ejecutivo

Todo el mundo reconoce que el sistema de autopistas y los automóviles son esenciales para el comercio. Pero es sólo ahora que las personas están empezando a entender cómo los sistemas informáticos compuestos por los computadores y las redes son otra infraestructura también esencial para el comercio. Al reconocer el rol fundamental que juegan los sistemas informáticos en las actividades de negocio de la Empresa X, esta política define las reglas y demás requisitos necesarios para la operación segura y confiable de la infraestructura de sistemas informáticos de la Empresa X.

Así como todo conductor juega un papel en la operación ordenada y segura de la infraestructura del transporte, de la misma manera existen roles y responsabilidades de seguridad informática para todos los empleados de la Empresa X. Por ejemplo, es responsabilidad del conductor reportar accidentes y es responsabilidad del empleado reportar problemas de seguridad informática. Así como los fabricantes de automóviles necesitan dotar a los vehículos de cinturones de seguridad, los diseñadores de sistemas de la Empresa X deben incluir medidas indispensables de seguridad, tales como restricciones de acceso a los usuarios en base a la necesidad de conocer.

Esta política también define un lineamiento básico de las medidas de control que se espera que todos los empleados de la Empresa X conozcan y sigan consistentemente. Algunas veces denominadas normas de controles de debido cuidado, estas medidas de seguridad son el mínimo requerido para evitar una serie de problemas que incluyen fraude y desfalco, espionaje industrial, sabotaje, errores y omisiones y no disponibilidad del sistema. Estas políticas también definen el mínimo de controles requeridos para evitar problemas legales como alegatos por negligencia, ruptura de la obligación fiduciaria o violación de la privacidad. Este documento detalla las vías razonables y prácticas para que todos en la Empresa X eviten pérdidas innecesarias.

La Empresa X depende en forma crítica de la continua confianza de sus clientes. Esta confianza se ha ganado poco a poco y es el resultado de muchos años de dedicado esfuerzo de los empleados de la Empresa X. Si bien crece lentamente, esta confianza puede perderse

rápidamente debido a problemas como intrusiones de hackers que provoquen caídas en el sistema. La confianza que depositan los clientes en la Empresa X es una ventaja competitiva que debe ser nutrida y fortalecida con esfuerzos como el de la seguridad informática.

Introducción

Función Crítica para el Negocio—La información y los sistemas informáticos son necesarios para la ejecución de casi todas las actividades esenciales de la Empresa X. Si se presentara un problema serio de seguridad con esta información o con estos sistemas informáticos, la Empresa X sufriría serias consecuencias, incluyendo la pérdida de clientes, reducción en las ganancias y se vería afectada su reputación. Como consecuencia, la seguridad informática debe ser una parte crítica del ambiente de negocios de la Empresa X.

Apoyo a los Objetivos del Negocio—Este documento de los requisitos de seguridad informática ha sido elaborado para garantizar que la Empresa X está en capacidad de mantener un crecimiento futuro del negocio y asegurar un nivel consistentemente alto de atención a sus clientes, proveedores, empleados y socios de negocios. Este documento también tiene como propósito mantener la reputación de la organización en la obtención de negociaciones de alta integridad y alta calidad. Debido a que la prevención de problemas de seguridad es considerablemente menos costosa que la corrección y recuperación, este documento ayudará a bajar los costos a largo plazo.

Esencial el Cumplimiento Constante—Una sola excepción no autorizada en las medidas de seguridad puede amenazar a otros usuarios, a la organización completa e inclusive a otras organizaciones externas, como los socios de negocios. La interconexión de los sistemas informáticos requiere que todos los empleados observen un mínimo de medidas de seguridad. Este documento define el mínimo nivel de controles adecuados. En algunos casos, estos requisitos entrarán en colisión con otros objetivos, tales como mejorar la eficiencia y minimizar los costos. La alta gerencia ha examinado estos equilibrios y ha determinado que los requisitos mínimos definidos en este documento son apropiados para todos los empleados de la Empresa X. Como condición para la estabilidad laboral, todos los

empleados, contratistas, consultores y empleados temporales, deben cumplir consistentemente los requisitos expuestos en este documento.

Se Requiere Esfuerzo en Equipo—Las herramientas disponibles en el campo de la seguridad informática son relativamente poco sofisticadas. Muchas de las tareas requeridas no pueden llevarse a cabo con los productos que se encuentran actualmente en el mercado. Esto significa que los usuarios en la Empresa X deben dar un paso hacia delante y jugar un papel importante en el área de seguridad informática. Ahora que la información y los sistemas informáticos están distribuidos en los computadores de la oficina y son utilizados en ubicaciones remotas, el papel del empleado se ha convertido en parte esencial de la seguridad informática. La seguridad informática no es dominio exclusivo del departamento de Sistemas Informáticos, sino un esfuerzo en equipo que requiere de la participación de todo empleado que está en contacto con la información o con los sistemas informáticos de la Empresa X.

Responsabilidades en Seguridad Informática

Propietarios de la Información—Los gerentes de nivel medio en los departamentos usuarios deben ser designados Propietarios de todas las clases de información utilizadas para las actividades cotidianas del negocio. Cada clase de "sistema informático de producción" debe tener un Propietario. Cuando los Propietarios de la información no se encuentran claramente definidos en el diseño organizacional, el ejecutivo jefe de información hará la designación. Los Propietarios de la información no poseen legalmente la información. Son integrantes del equipo gerencial de la Empresa X que toma decisiones en beneficio de la organización. Los Propietarios de la información o sus delegados deben tomar las siguientes decisiones y llevar a cabo las siguientes actividades:

- Aprobar privilegios de control de acceso a la información para perfiles específicos de trabajo.
- Aprobar solicitudes de control de acceso a la información que no se encuentran dentro del rango existente de perfiles de trabajo.
- Seleccionar un período de retención de datos para su información, en base a la recomendación del departamento Legal.
- Designar una fuente originaria de información a partir de la cual se deriven todos los informes gerenciales.

- Seleccionar los controles específicos necesarios para proteger la información, como cheques adicionales para validación de las entradas o procedimientos de respaldo más frecuentes.
- Definir límites aceptables de calidad de su información, como la exactitud, oportunidad y tiempo transcurrido entre la recopilación y el uso.
- Aprobar todos los usos nuevos y diferentes de su información.
- Aprobar todos los sistemas de aplicaciones nuevos o sustancialmente mejorados que utilicen su información antes de que estos sistemas tengan estatus operativo de producción.
- Revisar los informes acerca de intrusiones en el sistema y otra clase de eventos que afecten su información.
- Revisar y corregir informes que indiquen los usos actuales en producción de su información.
- Revisar y corregir informes que indiquen los perfiles de trabajo que tienen actualmente acceso a su información.
- Seleccionar una categoría de clasificación de acuerdo a la confidencialidad de su información, y revisar dicha clasificación cada cinco años para efectuar posibles degradaciones.
- Seleccionar una categoría de criticidad para su información de forma que pueda llevarse a cabo la apropiada planificación de contingencia.

Los Propietarios de la información deben designar un Propietario suplente que los pueda reemplazar en caso de ausentarse o no estar disponibles. Los Propietarios no deben delegar las responsabilidades de propiedad a terceros, como por ejemplo las organizaciones contratadas o una persona que no sea un empleado a tiempo completo de la Empresa X. Cuando ni el Propietario ni el Propietario suplente están disponibles, las decisiones inmediatas del Propietario las puede tomar el gerente del departamento que generalmente maneja la información.

El Gerente del Trabajador—Los Propietarios no aprueban las peticiones ordinarias de control de acceso. Es el gerente inmediato del trabajador quien debe aprobar la solicitud de acceso al sistema con base en los perfiles de trabajo existentes. Si un perfil de trabajo no existe, es responsabilidad del gerente crearlo, obtener la aprobación de los Propietarios pertinentes y notificar al departamento de Seguridad Informática. Cuando un

empleado abandona la Empresa X, es responsabilidad de su gerente inmediato informar inmediatamente al departamento de Seguridad Informática que los privilegios asociados con el identificador de dicho usuario deben ser revocados. Los identificadores de usuario son específicos para cada individuo y no deben ser reasignados o utilizados por otros. Poco después de la separación del empleado de la Empresa X, el gerente también es responsable de reasignar sus tareas y sus archivos a otros empleados.

Custodios de la Información—Los Custodios tienen posesión física o lógica de la información y de los sistemas informáticos. Los Custodios son designados específicamente para diferentes clases de información. En muchos casos, un gerente del departamento de Sistemas Informáticos actuará como el Custodio. Si no está claro quién es el Custodio, en función de las disposiciones operativas para los sistemas informáticos existentes, entonces el jefe ejecutivo de información hará la designación. Los Custodios siguen las instrucciones de los Propietarios, operan los sistemas en beneficio de los Propietarios, pero también sirven a los usuarios autorizados por los Propietarios. Los Custodios deben definir las opciones técnicas, como las categorías de criticidad de la información, y permitir que los Propietarios seleccionen la opción apropiada para su información. Los Custodios también definen las arquitecturas de los sistemas informáticos y proveen de asistencia de consultoría técnica a los Propietarios de forma tal que los sistemas informáticos puedan ser construidos y ejecutados para cumplir de la mejor manera con los objetivos del negocio. De ser requerido, los Custodios adicionalmente proporcionan informes a los Propietarios acerca de las operaciones del sistema informático y de problemas en la seguridad informática. Los Custodios son responsables de salvaguardar la información en su posesión, incluyendo la implantación de sistemas de control de acceso para evitar la divulgación inapropiada y el desarrollo, documentación y prueba de los planes de contingencia para los sistemas informáticos.

Usuarios de la Información—Los usuarios no son designados específicamente; sin embargo, están ampliamente definidos como todo empleado que tiene acceso a información interna o a sistemas informáticos internos. Los usuarios deben seguir todos los requisitos de seguridad definidos por los Propietarios, implementados por los Custodios o establecidos por el departamento de Seguridad Informática. Los usuarios deben familiarizarse y actuar en concordancia con todos los requisitos de seguridad informática de la Empresa X. Los usuarios

también deben participar en los esfuerzos de adiestramiento y concientización en seguridad informática. Los usuarios deben solicitar el acceso a través de su gerente inmediato e informar cualquier actividad sospechosa o problema de seguridad. Para más información acerca de los usuarios de información, ver “[Reporte de Problemas](#)” en la página 527.

Departamento de Seguridad Informática—El departamento de Seguridad Informática es el punto central de contacto para todos los asuntos relacionados con la seguridad informática en la Empresa X. Al actuar como consultores técnicos internos, es responsabilidad de este departamento crear compromisos de seguridad informática que consideren las necesidades de usuarios, Custodios, Propietarios y de terceros específicos. Al reflejar estos compromisos, este departamento define las normas de seguridad informática, procedimientos, políticas y demás requisitos aplicables a toda la organización. La Seguridad Informática debe manejar todas las actividades de administración del control de acceso, monitorear la seguridad de los sistemas informáticos de la Empresa X y proporcionar adiestramiento en seguridad informática y programas de concientización a los empleados de la Empresa X. El departamento es responsable de suministrar informes periódicamente a la gerencia acerca del estado actual de la seguridad informática en la Empresa X. Mientras que la planificación de contingencia para los sistemas informáticos es responsabilidad de los Custodios de la información, el departamento de Seguridad Informática debe proporcionar asistencia de consultoría técnica en relación con procedimientos de respuesta ante emergencias y recuperación de desastres. El departamento de Seguridad Informática también es responsable de organizar un equipo de respuesta ante emergencias computacionales para responder rápidamente a infecciones por virus, irrupciones de hackers, caídas del sistema y demás problemas de seguridad informática.

Departamento de Auditoría Interna—El departamento de Auditoría Interna de la Empresa X lleva a cabo periódicamente verificaciones de conformidad, para asegurar que todas las partes están llevando a cabo las tareas que les fueron asignadas, y para asegurar que los requisitos de seguridad informática están siendo respetados consistentemente. El Auditor Interno actúa como los ojos y oídos de la alta gerencia en la Empresa X, asegurando que los controles internos, incluyendo aquellos relacionados con la seguridad informática, son consistentes con las expectativas de la alta gerencia y con las metas organizacionales.

Clasificación de la Sensibilidad de la Información

Razones para Clasificar—Para el manejo adecuado de la información debe utilizarse a lo largo de toda la Empresa X una jerarquía de clasificación de acuerdo con su grado de sensibilidad. Esta jerarquía proporciona una manera rápida para referirse a la confidencialidad de la información y puede utilizarse para simplificar las decisiones de seguridad informática y minimizar sus costos. Un propósito importante de un sistema de clasificación de acuerdo con la confidencialidad es proveer un manejo consistente de la información sin importar la forma que tome, a donde vaya ni quién la posea. Es por esta razón que es importante mantener las etiquetas que reflejan las categorías de clasificación de acuerdo al grado de sensibilidad. La Empresa X utiliza cuatro categorías de clasificación:

Pública—Esta información ha sido específicamente autorizada para su divulgación al público por el departamento de Relaciones Públicas o por los gerentes del departamento de Mercadeo. La divulgación no autorizada de esta información no le causará problemas a la Empresa X, a sus clientes ni a sus socios de negocio. Como ejemplo se tienen los folletos de mercadeo y el material desplegado en la página web de la Empresa X. La divulgación al público de información de la Empresa X requiere de la existencia de esta etiqueta, el permiso específico del Propietario de la información o la práctica sostenida de distribución pública de esta información.

Sólo para Uso Interno—Esta información solamente se debe utilizar dentro de la Empresa X y, en algunos casos, dentro de organizaciones afiliadas como los socios de negocio de la Empresa X. La divulgación no autorizada de esta información a personas externas puede estar en contra de las leyes y reglamentos o puede causar problemas a la Empresa X, a sus clientes o a sus socios de negocio. Este tipo de información se encuentra ampliamente distribuida dentro de la Empresa X o puede ser distribuida dentro de la organización sin la autorización previa del Propietario de la información. Como ejemplos se tienen el directorio telefónico de la Empresa X y la mayoría de los mensajes de correo electrónico.

Confidencial—Esta información es privada o delicada por naturaleza y debe ser restringida a aquellos que tengan una necesidad legítima de negocios de acceder a ella. La divulgación no autorizada de esta información a personas que no tengan esa necesidad real de conocimiento puede estar en contra de las leyes y reglamentos o puede causar serios problemas a la Empresa X, a sus clientes o a sus socios de negocio. Las

decisiones acerca del otorgamiento de acceso a esta información deben ser clarificadas por el Propietario de la misma. Como ejemplos se tienen la información de las cuentas de los clientes en el momento de las transacciones y los registros de las evaluaciones de desempeño de los empleados.

Secreta—Esta información es la más privada y delicada y debe ser monitoreada y controlada todo el tiempo. La divulgación no autorizada de esta información a personas que no tengan una necesidad de negocio de acceder a ella, puede estar en contra de las leyes y reglamentos o puede causar severos problemas a la Empresa X, a sus clientes o a sus socios de negocio. Las decisiones acerca del otorgamiento de acceso a esta información deben ser clarificadas por el Propietario de la misma. Como ejemplos se tienen los planes de fusión o adquisición e información legal protegida por el privilegio abogado-cliente.

Categoría Predeterminada—Si la información no está marcada con ninguna de estas categorías, corresponderá por omisión en la categoría de Sólo para Uso Interno. Si la información cae dentro de esta categoría, no es necesario aplicar una etiqueta de confidencialidad. La información que se encuentra dentro de las categorías de Confidencial o Secreta es designada como Confidencial.

Etiquetado—El Propietario o creador de la información debe asignar una etiqueta apropiada, y el usuario o destinatario de esta información debe mantener consistentemente la etiqueta asignada. Las etiquetas para la información confidencial deben especificarse en el campo de Asunto para los mensajes de correo electrónico o en los memos en papel. Estas etiquetas deben encontrarse en la parte externa de los discuetes, carretes de cintas magnéticas, CD-ROMs, cassetes de audio y demás medios de almacenamiento. Si el medio de almacenamiento, digamos un disquete, contiene información con clasificaciones múltiples, la categoría más confidencial debe indicarse en la etiqueta externa. De la misma manera, cuando se crea una colección de información de fuentes con diferentes clasificaciones, la colección debe ser clasificada de acuerdo con el mayor nivel de sensibilidad de la información fuente.

Manejo de las Instrucciones—Todos los usuarios deben cumplir los requisitos para el manejo de la información en función de su sensibilidad. Para mayor información acerca de estas definiciones ver Capítulo 17, “[Modelo de Tabla de Referencia Rápida de Clasificación de Datos](#). Los Propietarios pueden asignar controles adicionales para restringir el acceso o para proteger su información.

Control de Acceso

Filosofía del Acceso—El acceso a la información Pública y Uso Interno Solamente no está restringido con controles de acceso que discriminan en función de un usuario específico. Por ejemplo, la información Pública está disponible en la página web de la Empresa X y la información Sólo para Uso Interno está disponible en la red interna de la Empresa X. El acceso a la información Confidencial o Secreta debe ser otorgado solamente cuando se ha demostrado la necesidad legítima de negocio y el acceso ha sido previamente aprobado por el Propietario de la información. El acceso a hardware y software específicos está restringido en función de la necesidad de negocios.

Proceso de Aprobación del Acceso—El gerente del empleado debe iniciar el proceso de aprobación del acceso y los privilegios otorgados permanecen vigentes hasta que el empleado cambie sus funciones o abandone la Empresa X. Si cualquiera de estos eventos ocurre, el gerente debe notificar inmediatamente al departamento de Seguridad Informática. Todos los no empleados, contratistas, consultores, empleados temporales y organizaciones subcontratadas deben pasar por un proceso similar de solicitud de acceso y autorización iniciado por el gerente de proyecto. Los privilegios de éstos deben ser revocados inmediatamente por el departamento de Seguridad Informática tan pronto culmine el proyecto o cuando los no empleados dejen de trabajar para la Empresa X. El gerente del proyecto pertinente es responsable de revisar la necesidad de la continuidad de los privilegios a los no empleados cada tres meses.

Facilidades Predeterminadas—De manera predeterminada, todos los usuarios reciben servicios básicos en los sistemas informáticos, tales como las facilidades de correo electrónico y acceso a procesadores de palabras. Estas facilidades básicas varían de acuerdo con el trabajo y se determinarán conjuntamente por los departamentos de Seguridad Informática y de Sistemas Informáticos. Todas las demás capacidades del sistema deben ser proporcionadas a través de los perfiles de trabajo o a través de una petición especial dirigida al Propietario pertinente de la información. La existencia de ciertos privilegios de acceso no significa que una persona esté autorizada a utilizarlos. Si los usuarios tienen preguntas acerca de los privilegios de control de acceso deben dirigirlas al departamento de Seguridad Informática.

Salidas de la Empresa X—Cuando un usuario abandona la Empresa X, todos sus privilegios informáticos y el acceso a la información de la Empresa

X deben cesar inmediatamente. Por ejemplo, los usuarios cesantes no pueden continuar manteniendo una cuenta de correo electrónico en la Empresa X. En este momento, toda la información de la Empresa X que fue divulgada a los usuarios debe ser devuelta o destruida. Por ejemplo, las listas de contacto de los clientes deben permanecer en la Empresa X. Todo el trabajo realizado por los usuarios para la Empresa X es propiedad de la misma y también debe permanecer dentro de ella cuando los usuarios se van. Por ejemplo, un programa de computación escrito por un integrante del departamento de Sistemas Informáticos mientras formaba parte de la Empresa X es propiedad de la misma y debe permanecer en ella.

Identificador Único de Usuario—Cada usuario debe ser asignado su propio y único identificador de usuario. Este identificador va junto con la persona cuando se mueve a lo largo de la organización y debe ser desactivado cuando el usuario sale de la Empresa X. No está permitida la reutilización de las identificaciones de usuario. Cada identificador de usuario y su contraseña son específicos para el uso de una persona en particular. A pesar de que los identificadores de usuario pueden ser comunicados en los mensajes de correo electrónico y en otros lugares, las contraseñas nunca deben ser compartidas con nadie. Los técnicos de sistemas informáticos tienen todos los privilegios que requieren para llevar a cabo su trabajo y nunca deben obtener la contraseña de un usuario. Los identificadores de usuario están asociados a personas específicas y no a terminales de computadores, departamentos o posiciones de trabajo. Con excepción de las páginas en Internet, Intranet y demás ubicaciones en donde la interacción anónima es generalmente entendida y esperada, los identificadores de usuarios anónimos y de invitados no están permitidos, a menos que hayan sido autorizados previamente por el departamento de Seguridad Informática.

Desactivación de Privilegios—Después de un período de inactividad definido en minutos por el departamento de Seguridad Informática, las sesiones en línea con máquinas multiusuario deben ser terminadas automáticamente. Los usuarios deben desconectarse de los computadores multiusuario cuando salen de sus oficinas por un lapso de tiempo mayor a algunos minutos. Los identificadores de usuario que permanecen inactivos en computadores multiusuario y que no tienen actividad por un período definido en semanas por el departamento de Seguridad Informática deben perder automáticamente sus privilegios y archivar la documentación correspondiente. Los usuarios que retornan de una vacación prolongada o de un permiso remunerado deben

pedir a su gerente que contacte al departamento de Seguridad Informática para que restablezca sus privilegios.

Autenticación de Usuarios—Todos los identificadores de usuario de los sistemas informáticos de producción deben tener una contraseña asociada o un mecanismo más fuerte, como una tarjeta de contraseña dinámica, para garantizar que únicamente el usuario autorizado pueda utilizar el identificador de usuario. Los usuarios son responsables de toda la actividad que ocurra con su identificador y contraseña u otro mecanismo de autenticación. Un usuario debe cambiar su contraseña inmediatamente si sospecha que ha sido descubierta por otra persona. Los usuarios deben notificar al departamento de Seguridad Informática si se han violado otros mecanismos de control o si sospechan que estos mecanismos se han visto comprometidos.

Gestión de Contraseñas Fijas

Selección de Contraseñas—Los usuarios deben seleccionar contraseñas difíciles de adivinar. Las contraseñas fijas no deben encontrarse en el diccionario y no deben hacer mención de la vida privada del usuario. Todas las contraseñas fijas deben tener al menos 10 caracteres y esta longitud mínima debe ser reforzada automáticamente por los sistemas que la soportan. Los usuarios deben escoger contraseñas que incluyan tanto caracteres alfabéticos como numéricos.

Cambio de Contraseñas—Las contraseñas seleccionadas por los usuarios no pueden ser reutilizadas o recicladas. Cuando los sistemas lo soporten, las contraseñas fijas deben ser modificadas cada 60 días y deben ser cambiadas la primera vez que se utilicen. Si un usuario sospecha que alguien más conoce su contraseña, debe cambiarla inmediatamente. El Centro de Atención al Usuario del departamento de Seguridad Informática no reiniciará las contraseñas de los usuarios a menos que el usuario se identifique.

Protección de Contraseñas—Los usuarios no deben compartir las contraseñas fijas con nadie, incluyendo gerentes y compañeros. Los usuarios emplearán mecanismos autorizados para compartir información como los directorios en los servidores locales, correo electrónico, páginas en Intranet o discuetes. Los usuarios no deben almacenar las contraseñas fijas en ningún archivo de computador, tales como programas reducidos de inicio de sesión o programas de computación, a menos que las contraseñas hayan sido cifradas con un software autorizado para ello. Las contraseñas no pueden ser anotadas a menos que un proceso de transformación las haya ocultado, o que

estén seguras físicamente, como por ejemplo en un archivador bajo llave. Todas las contraseñas fijas predeterminadas suministradas por el proveedor de hardware o software deben ser cambiadas antes de que el sistema pueda ser utilizado en las actividades de negocio de la Empresa X

Privacidad

Expectativas de Privacidad—Los usuarios no deben tener expectativas de privacidad cuando utilicen los sistemas informáticos de la Empresa X. Para manejar los sistemas y reforzar la seguridad, la Empresa X puede registrar, revisar y utilizar cualquier información almacenada o que pase a través de sus sistemas. La Empresa X puede monitorear la actividad del usuario, tales como los números telefónicos marcados y las páginas web visitadas.

Recopilación de Información—La Empresa X no recopila información no necesaria para sus fines de negocio. Tampoco recopila información de terceros, como los clientes, a menos que éstos sean notificados acerca de las actividades de recopilación antes de que ocurran.

Privacidad de la Información de Terceros—Una gran variedad de terceros ha confiado su información a la Empresa X con fines de negocio y todos los trabajadores de la Empresa X deben hacer lo máximo para salvaguardar la privacidad y seguridad de esta información. Los datos de la cuenta de los clientes es Confidencial y el acceso debe estar estrictamente limitado a la necesidad del negocio. La información de la cuenta del cliente no puede ser distribuida a terceros sin una autorización previa del cliente. Se harán excepciones en caso de incapacidad o fallecimiento del cliente.

Divulgaciones a Terceros

Autorización Previa para Declaraciones Públicas—Todos los trabajadores que deban efectuar discursos, escribir documentos o divulgar información acerca de la Empresa X o de sus negocios, requieren de una autorización previa del departamento de Relaciones Públicas. Únicamente las personas designadas están autorizadas para ser voceros de la Empresa X. A menos que un trabajador sea el vocero designado, todas las preguntas de los medios deben ser dirigidas al departamento de Relaciones Públicas.

Acuerdos de Confidencialidad de la Empresa X—Cada vez que las comunicaciones con terceros requieran el despliegue de información delicada de la

Empresa X, un acuerdo de confidencialidad (NDA, por sus siglas en inglés) debe ser firmado por el tercero. La información divulgada a estos terceros estará limitada a los aspectos relacionados directamente con el proyecto involucrado o con la relación de negocios, y la divulgación debe estar previamente autorizada por el Propietario pertinente de la información.

Acuerdos de Confidencialidad de Terceros—En algunos casos, antes de comenzar las discusiones, los terceros pueden exigir que los trabajadores de la Empresa X firmen sus acuerdos de confidencialidad (NDA). Los receptores de estos NDA de terceros deben enviar estos acuerdos al departamento Legal. Estos acuerdos deben ser firmados únicamente por integrantes del departamento Legal de la Empresa X.

Uso Aceptable de Internet

No Es un Beneficio Laboral—El acceso a Internet más allá del correo electrónico debe ser proporcionado únicamente si es necesario para realizar el trabajo del trabajador. Si el usuario requiere acceso adicional a los servicios de Internet, debe hacer una solicitud a su gerente, quien debe contactar al departamento de Seguridad Informática.

Confiabilidad de la Información—Toda la información obtenida de Internet debe ser considerada sospechosa hasta que se confirme con información proveniente de otra fuente confiable. Los usuarios no deben confiar en la identidad supuesta de un corresponsal en Internet, a menos que la identidad de esta persona sea confirmada a través de métodos autorizados por el departamento de Seguridad Informática, como por ejemplo certificados o firmas digitales.

Despliegue de Información a Grupos de Discusión—Los usuarios no deben publicar información en grupos de discusión públicos, sitios para conversación u otra clase de foros públicos en Internet a menos que hayan sido previamente autorizados por el departamento de Relaciones Públicas para representar a la Empresa X. La gerencia se reserva el derecho a remover cualquier información de Internet colocada por un trabajador que se considere inadecuada o potencialmente dañina para la reputación de la organización.

Descarga de Software—Los usuarios no deben descargar software de Internet a menos que estén específicamente autorizados para hacerlo por el departamento de Sistemas Informáticos o de Seguridad Informática. Los usuarios pueden descargar archivos de datos de Internet pero deben verificar que estos archivos

no tengan virus antes de ejecutarlos. Dependiendo del archivo, puede requerirse su descompresión o descifrado antes de proceder a descargarlo.

Envío de Parámetros de Seguridad—Los usuarios no deben enviar ningún parámetro confidencial, tales como números de tarjetas de crédito, números de tarjetas telefónicas, contraseñas fijas o números de cuenta del cliente, a través de Internet, a menos que la conexión esté cifrada. Los usuarios no deben incluir parámetros confidenciales en mensajes de correo electrónico enviados a través de Internet, a menos que estos mensajes estén cifrados con software autorizado por el departamento de Seguridad Informática. No es suficiente que un trabajador utilice una red privada virtual (VPN, por sus siglas en inglés) para conectarse con los computadores de la Empresa X, a pesar de que el resultado sea que el enlace de comunicación entre el computador remoto y los computadores de la Empresa X quede cifrado. El uso de una VPN permite que un mensaje de correo electrónico enviado a un tercero fuera de la empresa pueda viajar a través de enlaces cifrados. Los parámetros de seguridad no deben enviarse a través del correo electrónico a terceros fuera de la empresa a menos que se utilice el cifrado en ambas vías.

Transferencia Internacional de Datos—El traslado internacional de información privada, como por ejemplo los registros de recursos humanos, se considera ilegal en algunos países. Antes de transferir cualquier clase de información privada fuera del país, los usuarios deben verificar que el departamento de Seguridad Informática se asegure de que no se están violando las leyes.

Establecimiento de Servicios Adicionales—La suscripción a servicios en Internet de distribución automática de información en tiempo real debe ser autorizada por el departamento de Sistemas Informáticos. La suscripción a distribución de listas por correo electrónico es permisible sin autorización previa. El establecimiento de cualquier conexión en red con un tercero está prohibido, a menos que el departamento de Seguridad Informática haya autorizado los controles asociados con esta conexión. Los usuarios no deben producir páginas web, boletines electrónicos ni ningún otro mecanismo que permita el acceso público a información acerca de la Empresa X sin la autorización previa tanto del departamento de Seguridad Informática como del departamento de Relaciones Públicas. El establecimiento de intercambio electrónico de datos y de cualquier otro sistema electrónico de negocios está prohibido a menos que haya sido autorizado por el departamento de Seguridad Informática y por el departamento de Relaciones Públicas.

Anonimato del Usuario: Los usuarios no deben tergiversar, oscurecer, suprimir o reemplazar su propia identidad o la de otro usuario en Internet o en cualquier otro sistema informático de la Empresa X. En todas las instancias, el nombre del usuario, la dirección de correo electrónico, la afiliación organizacional y demás información de contacto, deben reflejar quién origina el mensaje o el anuncio. Está prohibido el uso de correos anónimos o de otros mecanismos para ocultar la identidad. Esta permitido el uso de exploradores web, protocolos de transferencia de archivos con usuarios anónimos y demás métodos establecidos para los que los usuarios no necesitan identificarse.

Reportes de Seguridad Falsos—Todos los usuarios que reciban información acerca de las vulnerabilidades del sistema deben enviar dicha información al departamento de Seguridad Informática, donde se determinarán las medidas apropiadas al respecto. Los usuarios no deben redistribuir información sobre las vulnerabilidades del sistema.

Establecimiento de Conexiones en Red

Los computadores o redes de la Empresa X pueden ser conectados a computadores o redes de terceros únicamente después de que el departamento de Seguridad Informática haya determinado que los sistemas combinados cumplen con los requisitos de seguridad de la Empresa X. Las conexiones en tiempo real entre dos o más sistemas de computación internos de la Empresa X no pueden establecerse hasta que el departamento de Seguridad Informática haya determinado que estas conexiones no amenazarán la seguridad informática. Las conexiones de computadores internos de la Empresa X con la red interna de la Empresa X no requieren esta clase de permisos, a menos que los sistemas involucrados almacenen información confidencial. Las conexiones a Internet a través de cortafuegos de la Empresa X no requieren esta clase de permisos.

Los trabajadores no deben conectar sus propios computadores con los computadores o redes de la Empresa X sin una autorización previa del jefe de su departamento. Los sistemas que pertenezcan a particulares no deben ser utilizados para procesar ninguna clase de información de la Empresa X a menos que su uso haya sido autorizado por el departamento de Seguridad Informática.

Los trabajadores y proveedores de la Empresa X no deben hacer arreglos para instalar o finalizar la instalación de líneas de voz o de datos con ninguna telefónica, a menos que tengan la autorización escrita del director del departamento de Telecomunicaciones.

Todas las conexiones entre las redes internas de la Empresa X e Internet o cualquier otra red de acceso público deben tener un cortafuego autorizado o un sistema de control de acceso. Los privilegios autorizados a través de este cortafuego o sistema de control de acceso deben basarse en las necesidades del negocio o deben definirse de acuerdo con una norma de control de acceso elaborada por el departamento de Seguridad de Sistemas Informáticos [debe insertarse un enlace a ese documento aquí].

Acceso Discado

Con excepción de los computadores portátiles y computadores con conexión de teletrabajo, está prohibido el uso de módems internos o conectados a computadores personales para establecer sesiones de comunicación con computadores o redes de la Empresa X. Todas las conexiones discadas con computadores y redes de la Empresa X deben ser dirigidas a través de un módem que incluye un sistema de seguridad de autenticación extendida del usuario autorizado por el departamento de Seguridad Informática.

Acceso de Terceros

Antes de que se permita el acceso de terceros a los sistemas internos de la Empresa X a través de conexiones en tiempo real, debe obtenerse una autorización específica por escrito del gerente del departamento de Seguridad Informática. Entre estos terceros se incluyen los proveedores de información como organizaciones contratadas, socios de negocios, contratistas y consultores que trabajan en proyectos especiales.

A los proveedores de sistemas informáticos se deben otorgar solamente privilegios de conexión entrante cuando el gerente de sistemas determina que efectivamente existe necesidad legítima del negocio. Estos privilegios están activos únicamente por el período de tiempo requerido para llevar a cabo las tareas previamente definidas y autorizadas. El departamento de Seguridad Informática debe dar su autorización en caso de que el acceso del proveedor sea superior a un día.

A menos que el Propietario de la información haya dado su autorización previa, los trabajadores no deben colocar sino información pública de la Empresa X en un directorio, servidor o en cualquier otra ubicación en donde personas desconocidas puedan tener acceso.

Como condición para poder acceder a la red de la Empresa X, todo tercero debe asegurar sus propios sistemas de conexión de forma consistente con los requisitos de la Empresa X. La Empresa X se reserva el

derecho de auditar las medidas de seguridad en los sistemas conectados con terceros sin previo aviso. También se reserva el derecho a terminar inmediatamente las conexiones de red con todos los sistemas de terceros que no cumplan estos requisitos.

Cifrado

No Existe Protección Predeterminada—Las redes de la Empresa X, Internet y otras redes públicas no están protegidas de manera predeterminada contra la intervención telefónica. En la mayoría de los casos, si la información debe ser protegida, el usuario debe tomar acciones específicas para hacer posible el cifrado. Los usuarios que utilizan celulares o teléfonos móviles no deben discutir información Confidencial o Secreta a menos que hayan tomado los pasos para cifrar la llamada. Las videoconferencias no deben involucrar la discusión de información delicada a menos que estén activadas las facilidades de cifrado.

Cuándo Utilizar el Cifrado—Siempre que se envíe información Confidencial o Secreta a través de una red pública como Internet, deben utilizarse los métodos de cifrado autorizados por el departamento de Seguridad Informática para proteger dicha información. Cuando la información Secreta se almacena en un computador, este almacenamiento debe hacerse utilizando métodos similares de cifrado ya autorizados. Para obtener más información acerca de estas circunstancias, ver Capítulo 17, “[Modelo de Tabla de Referencia Rápida de Clasificación de Datos](#).”

Selección de las Claves—Muchas rutinas de cifrado requieren que el usuario provea una semilla o una clave como entrada. Los usuarios deben proteger estos parámetros de seguridad de la divulgación no autorizada de la misma manera que protegen las contraseñas. Las reglas para seleccionar claves sólidas deben ser las mismas que para seleccionar contraseñas sólidas.

Correo Electrónico

Compartir y Enviar—Las cuentas de correo electrónico, al igual que los identificadores de usuarios, son específicas para individuos y no deben ser compartidas. Si un usuario sale de vacaciones o no puede consultar su correo durante un largo lapso de tiempo, los mensajes pueden ser enviados a otro trabajador de la Empresa X. Se pueden enviar notificaciones que informen automáticamente a los remitentes que el destinatario no responderá durante un determinado periodo de tiempo. Al salir de la Empresa X, la cuenta de correo electrónico del usuario debe ser terminada. No se permite el envío de correo electrónico a direcciones fuera de la Empresa X. Si un mensaje de correo electrónico contiene información confidencial, los usuarios no lo deben enviar a otro destinatario a menos que esté autorizado para conocer la información o que su originador apruebe el envío. La facilidad de envío de mensajes de correo electrónico propagados no debe ser empleada, a menos que se obtenga la autorización del gerente del departamento; sin embargo, el uso de listas seleccionadas de distribución es recomendable y permisible sin dicha autorización.

Protección Predeterminada—Los usuarios deben ser cuidadosos acerca de la inclusión de información delicada en mensajes de correo electrónico que no están protegidos con cifrado. Los usuarios deben emplear las facilidades del cifrado autorizadas por el departamento de Seguridad Informática.

Registro de Mensajes—Los usuarios son responsables de salvar mensajes importantes que puedan ser utilizados en el futuro. Los sistemas de correo electrónico no deben ser utilizados para almacenamiento de mensajes. Los usuarios deben mover los mensajes importantes de los sistemas de correo electrónico a otros sitios de almacenamiento, tales como los procesadores de palabras.

Contenido de los Mensajes—Los usuarios no deben utilizar expresiones profanas, obscenidades o anotaciones derogatorias en ningún mensaje de correo electrónico en el que se mencionen trabajadores, clientes, competidores y demás personas involucradas con el negocio de la Empresa X. Este tipo de anotaciones puede crear problemas legales como el libelo comercial y la demanda por difamación. Se exige especial cuidado debido a que los respaldos y las copias en archivos de mensajes de correo electrónico realizadas por terceros pueden de hecho ser más permanentes y más accesibles que las comunicaciones tradicionales en papel.

Acoso o Mensajes Ofensivos—Los sistemas informáticos de la Empresa X no se deben utilizar para el ejercicio del derecho del usuario a la libre expresión. El acoso sexual, étnico y racial, incluyendo llamadas telefónicas no solicitadas, mensajes de correo electrónico y de correo interno, está estrictamente prohibido. Los usuarios deben responder directamente al originador de mensajes ofensivos por correo electrónico, llamadas telefónicas u otras comunicaciones. Si el originador no deja rápidamente de enviar estos mensajes ofensivos, los trabajadores deben reportar las comunicaciones a su jefe y al departamento de Recursos Humanos.

Impresión, Fotocopiado y Transmisión por Fax

Destrucción de Copias de Desecho—Si una impresora, copiadora o máquina de fax se daña o funciona mal cuando está imprimiendo información Confidencial o Secreta, los usuarios involucrados no deben dejar la máquina hasta que todas las copias de la información delicada sean removidas o no sean legibles. Todas las copias en papel de información deben ser eliminadas con la destructora de papel o con cualquier otro método autorizado por el departamento de Seguridad Informática.

Precauciones al Enviar Comunicaciones por Fax—La información confidencial no debe ser enviada por fax, a menos que un integrante autorizado del equipo esté cerca en el momento de la transmisión, de manera que maneje adecuadamente la información en el lugar de recepción, o si el fax se envía a una habitación cerrada a la que únicamente los trabajadores autorizados tengan acceso o a un buzón de fax que esté protegido con una contraseña de forma que se restrinja la divulgación al destinatario autorizado. La información confidencial no puede enviarse por fax a través de intermediarios no confiables como los trabajadores de un hotel o el personal de servicios de alquiler de buzones de correo. La información Secreta puede ser enviada por fax únicamente si la conexión está protegida con sistemas de cifrado autorizados por el departamento de Seguridad Informática. La recepción de información confidencial enviada por fax debe ser rápidamente confirmada. Todos los mensajes por fax deben tener una página de portada tipo plantilla que incluya el lenguaje autorizado por el departamento Legal de la Empresa X. Las firmas de terceros en contratos, órdenes de compra y demás documentos legales enviados por fax deben siempre estar seguidas del intercambio de originales en papel.

Precauciones al Imprimir—Cuando se imprime información confidencial, el usuario debe estar presente en el momento de la impresión, de forma que se evite que ésta sea revelada a terceros no autorizados, o debe dirigir la impresión dentro de un área en donde solamente pueda entrar personal autorizado.

Precauciones al Fotocopiar—Salvo que se obtenga permiso del Propietario de los derechos de autor, está prohibido hacer copias de material de revistas, periódicos, gacetas y demás publicaciones, a menos que esté dentro de los parámetros de lo razonable y de lo acostumbrado. Para obtener más información acerca de la copia de programas y demás materiales ver “[Derechos de Propiedad Intelectual](#)” en la página 526.

Servicios de Reparaciones—La reparación de máquinas de fax, impresoras y copiadoras debe ser realizada únicamente por proveedores que hayan firmado un acuerdo de confidencialidad con la Empresa X.

Computación Móvil y Trabajo en Casa

Autorización para Acceso Remoto—El acceso remoto a computadores de la Empresa X debe ser otorgado únicamente a aquellos usuarios que tienen una necesidad de negocio demostrable para dicho acceso. El permiso para acceder a computadores de la Empresa X en forma remota es otorgado y revisado anualmente por el gerente del usuario. Todos los usuarios remotos deben asistir a una clase especial antes de recibir los privilegios de acceso remoto o su renovación anual. La Empresa X se reserva el derecho de realizar auditorías sorpresa a los usuarios que tengan privilegios de acceso remoto. Estas auditorías sorpresa pueden incluir visitas a los sitios remotos y revisión del contenido del computador utilizado para acceder los sistemas de la Empresa X.

Independencia de Ubicación—Todos los requisitos de seguridad se aplican a las ubicaciones remotas, a pesar de que pueden ser implementados de distintas maneras. Por ejemplo, la información Confidencial o Secreta en papel debe ser guardada bajo llave cuando no se esté utilizando. En las oficinas de la Empresa X, puede utilizarse un archivador, pero en la vía, puede emplearse un maletín con llave.

Paquetes de Control de Acceso—Todos los computadores portátiles y remotos que estén bajo el control de los trabajadores de la Empresa X y que se utilicen para procesar información de negocios de la Empresa X, deben estar protegidos con un paquete de control de acceso autorizado por el departamento de Seguridad

Informática. Estos paquetes de control de acceso deben evitar el uso no autorizado de estas máquinas y el acceso no autorizado a la información de la Empresa X. Estos paquetes deben prevenir infecciones por virus y demás clases de daños por software malicioso.

Manejo de Información Confidencial—La información delicada (Confidencial o Secreta) no debe abandonar las oficinas de la Empresa X. Si es necesario eliminar información confidencial legible por computador de las oficinas de la Empresa X, la información debe estar protegida con facilidades de cifrado autorizadas por el departamento de Seguridad Informática. Si se transmite información confidencial a través de redes públicas como Internet, esta transmisión debe hacerse utilizando facilidades de cifrado autorizadas por el departamento de Seguridad Informática. Todos los sistemas portátiles y remotos que almacenen información confidencial de la Empresa X deben también emplear sistemas de cifrado para el disco duro.

Autentificación de Usuarios Remotos—El acceso remoto a computadores y redes de la Empresa X requiere que todos los usuarios estén definitivamente autenticados con contraseñas dinámicas u otros sistemas de identificación autorizados por el departamento de Seguridad Informática. Todos los usuarios remotos deben conectarse a los computadores y redes internas de la Empresa X a través de sistemas autorizados de comunicación como los cortafuegos y módem. La conexión entrante a los computadores o redes de la Empresa X a través de un módem de la oficina está prohibida, a menos que se haya obtenido la autorización específica del departamento de Seguridad Informática. La conexión saliente a redes de terceros, incluyendo Internet, es permisible a través de módems. Está prohibido dejar los módems de computadores personales en el modo de respuesta automática a menos que se haya instalado un sistema de identificación remota del usuario, autorizado por el departamento de Seguridad Informática.

Robo de Equipos—Si el equipo de los sistemas informáticos utilizado para manejar información de la Empresa X no es almacenado en áreas cerradas, los usuarios deben utilizar equipo antirrobo autorizado por el departamento de Seguridad Informática. Los usuarios no deben almacenar contraseñas, identificadores de usuario, ni ninguna otra clase de información de acceso en sistemas portátiles o remotos. Las tarjetas de contraseñas dinámicas u otros mecanismos de control de acceso empleados para el acceso remoto, no deben almacenarse en el mismo estuche de los computadores portátiles.

Seguridad de Oficinas Remotas—Antes de la autorización para trabajar en casa o a través de computadores con conexión desde casa, el gerente del usuario debe revisar el ambiente de seguridad del medio propuesto de trabajo. Si el usuario trabaja con información confidencial, debe emplearse una destructora de papel provista por la Empresa X. Si la información confidencial se almacena en forma de papel, debe estar disponible un mueble con llave o una caja de seguridad provista por la Empresa X. Los usuarios deben garantizar que sus archivos serán respaldados en forma remota en la red o que poseen sistemas remotos para llevar a cabo sus propios respaldos.

Consideraciones sobre Viajes—Los usuarios deben ser cuidadosos y no conversar sobre información confidencial cuando se encuentren en lugares públicos, tales como los vestíbulos de los hoteles, restaurantes y ascensores. Está prohibido ver información confidencial en la pantalla de un computador o en un informe escrito en papel cuando el usuario se encuentra en un lugar público como un avión. Los usuarios deben ser cuidadosos y no proporcionar información confidencial en mensajes de correo de voz o mensajes en beepers alfanuméricos.

Virus, Software Malicioso y Control de Cambios

Obligatorio Software Antivirus—Sistemas antivirus autorizados por el departamento de Seguridad Informática deben ser instalados en todos los computadores personales con sistemas operativos susceptibles a virus, en todos los cortafuegos con conexiones a redes externas y en todos los servidores de correo electrónico. Todos los archivos que provienen de fuentes externas deben ser verificados antes de su ejecución o utilización. Si se han comprimido o cifrado los datos, estos procesos deben ser revertidos antes de que tenga lugar el proceso antivirus. Los usuarios no deben apagar o desactivar los sistemas antivirus.

Si se Detecta un Virus—Si los usuarios reciben alertas de virus, deben desconectarse inmediatamente de todas las redes y dejar de utilizar el computador infectado y llamar al Centro de Atención al Usuario de Sistemas Informáticos para solicitar asistencia técnica. Los usuarios no deben eliminar los virus. Si los usuarios piensan que han sido víctimas de otro software malicioso, deben contactar inmediatamente al asistente técnico para minimizar el daño. La posesión o desarrollo de virus u otra clase de software malicioso está prohibido.

Control de Cambios—Los usuarios no deben instalar sistemas operativos nuevos o actualizados o aplicaciones de software en computadores personales u otras máquinas utilizadas para procesar información de la Empresa X. Los sistemas utilizados para procesar información de la Empresa X pueden ser de su propiedad pero han sido específicamente reconocidos como sistemas utilizados para las actividades regulares de negocios. Este enfoque permite que la Empresa X distribuya programas en forma automática, maneje las licencias de software automáticamente, realice respaldos remotos automáticos, y demás funciones relacionadas sobre una base centralizada y coordinada. Dado que el control de cambios se mantendrá a través de los paquetes de control de acceso ya mencionados, los usuarios pueden, sin embargo, cambiar las preferencias de los paquetes de software, como por ejemplo los tipos de letra del procesador de palabras que utilicen.

Uso Personal de los Sistemas Informáticos

Uso Personal—Toda actividad del usuario está supeditada a su registro y posterior análisis. Los usuarios no deben llevar a cabo ninguna actividad en los sistemas informáticos de la Empresa X que pueda dañar la reputación de la misma. La conducta inapropiada puede conducir a acciones disciplinarias, incluyendo la revocación de los privilegios de acceso. El uso personal incidental de los sistemas informáticos de la Empresa X, incluyendo el teléfono, está permitido siempre y cuando no interfiera con el desempeño del trabajo, no niegue a otros usuarios el derecho a acceder a los recursos del sistema y no incurra en costos significativos. El uso personal de la información de la Empresa X, como la listas de correo, requiere la autorización previa del Propietario pertinente de la información. El uso de software con licencia para la Empresa X en un computador personal de un usuario no está autorizado, a menos que el sistema esté designado para procesar información de la Empresa X.

Prohibición de Pruebas—Los usuarios no deben probar o tratar de comprometer cualquier mecanismo de seguridad informática a menos que hayan sido específicamente autorizados para hacerlo por el departamento de Seguridad Informática. Los usuarios no deben poseer software u otras herramientas diseñadas para comprometer la seguridad informática.

Derechos de Propiedad Intelectual

Propiedad Legal—Con excepción del material que claramente pertenece a terceros, la Empresa X es el propietario legal de toda la información de negocios almacenada o que pasa por sus sistemas. A menos que el

jefe oficial de información haya firmado un acuerdo específico por escrito, toda la información relacionada con los negocios desarrollada mientras el usuario trabaja para la Empresa X es propiedad de la Empresa X.

Copiado de Software—Los usuarios no deben hacer copias o utilizar software a menos que estén conscientes de que las copias que están haciendo tienen la licencia del proveedor para la Empresa X. Si un sistema que es utilizado para procesar información de la Empresa X ha sido instalado por el departamento de Sistemas Informáticos, los usuarios pueden confiar en que todo el software que se encuentra en dicho sistema tiene licencia y está autorizado. Las preguntas acerca del licenciamiento deben dirigirse al departamento de Sistemas Informáticos que mantiene documentación que refleja las licencias de software a lo largo y ancho de la Empresa X. Son permitidos los respaldos regulares de software con propósitos de planificación de contingencias. Los Sistemas Informáticos deben eliminar todo software no autorizado de los sistemas que se utilizan para procesar información de la Empresa X.

Etiquetado—Además de mantener las etiquetas mencionadas en “[Clasificación de la Sensibilidad de la Información](#)” en la página 518, los usuarios deben mantener información acerca de la fuente, fecha, y restricciones de uso para toda la información proporcionada por terceros. Estas etiquetas serán importantes para la toma de decisiones de la gerencia y demostrarán que la Empresa X cumple las leyes de derecho de autor y de propiedad intelectual. Los usuarios deben asumir que todos los materiales en Internet tienen derecho de autor, a menos que exista una notificación específica que indique lo contrario.

Desarrollo de Sistemas

Definición de Sistema de Producción—Los sistemas informáticos que hayan sido designados sistemas de producción tienen requisitos de seguridad especiales. Un sistema de producción es un sistema que se utiliza regularmente para procesar información crítica para el negocio de la Empresa X. A pesar de que un sistema de producción puede ubicarse físicamente en cualquier lugar, su designación es realizada por el gerente de Operaciones del departamento de Sistemas Informáticos.

Requisitos Especiales de los Sistemas de Producción—Todo el software desarrollado internamente que se ejecuta en los sistemas de producción debe desarrollarse de acuerdo con la metodología del departamento de Sistemas Informáticos (SDM, por sus siglas en inglés). Esta metodología debe garantizar que el

software será documentado adecuadamente y probado antes de ser utilizado para manejar información crítica de la Empresa X. La SDM también debe garantizar que los sistemas de producción incluyen medidas de control adecuadas. Los sistemas de producción deben tener Propietarios y Custodios designados para la información crítica que procesan. La Seguridad Informática debe llevar a cabo evaluaciones periódicas de riesgo en los sistemas de producción para determinar si los controles empleados son los adecuados. Todos los sistemas de producción deben tener un sistema de control de acceso para restringir el acceso y los privilegios disponibles a ciertos usuarios. Para todos los sistemas de producción debe asignarse un administrador de control de acceso que no sea un usuario regular del sistema.

Separación entre Sistemas de Producción, Desarrollo y Prueba—Mientras que los recursos lo permitan, debe existir una separación entre los ambientes de producción, desarrollo y prueba. Cuando estas distinciones se han establecido, el personal de desarrollo y prueba no debe tener acceso a los sistemas de producción. Toda prueba del software de producción debe hacerse reemplazando la información Secreta o Confidencial por datos falsos. Todas las medidas de seguridad proporcionadas por los proveedores de software deben pasar por un proceso de prueba metodológica y deben ser instaladas rápidamente. Los programadores de aplicaciones no deben tener acceso a la información de producción. Debe utilizarse un proceso de cambio de control formal y documentado para restringir y autorizar cambios en los sistemas de producción. Todas las vías de acceso basadas en programas de aplicación distintas a las vías de acceso autorizadas para los usuarios deben ser eliminadas o desactivadas antes de que el software pase a producción.

Programación del Usuario—Los usuarios no deben escribir programas de computación para producción a menos que hayan sido específicamente autorizados por el jefe oficial de información. La construcción de hojas de cálculo, comandos de ejecución automática que se ejecutan cuando un sistema es inicializado, o las bases de datos, no son considerados en este documento como programación. Tanto los usuarios como programadores deben ser cuidadosos y nunca deben incluir en ningún archivo sus identificadores de usuario, contraseñas, claves de cifrado y demás parámetros de seguridad.

Reporte de Problemas

Qué Reportar—Todos los trabajadores deben informar rápidamente al departamento de Seguridad Informática cualquier pérdida o daño severo en su hardware o software. Los trabajadores deben reportar cualquier sospecha de que los sistemas informáticos de la Empresa X estén comprometidos. Deben reportar todas las vulnerabilidades conocidas de los sistemas informáticos. También deben ser reportados los casos de sospecha de divulgación de información Secreta o Confidencial.

Cómo Reportar—Se ha establecido una línea dedicada de correo de voz con alerta a un beeper para manejar los reportes de problemas de seguridad. Las personas que llamen a esta línea pueden dejar mensajes anónimos. Los reportes no deben enviarse a través de correo electrónico a menos que el mensaje se haya cifrado con software autorizado por el departamento de Seguridad Informática. Todos los reportes deben ser investigados antes de tomarse cualquier medida. Los trabajadores también pueden utilizar esta línea para formular preguntas sobre seguridad informática.

Situaciones de Incumplimiento

Aceptación del Riesgo—El incumplimiento de éste y otros requisitos de seguridad informática puede llevar a una acción disciplinaria que puede incluir el cese laboral. En raras ocasiones, puede aceptarse un caso de incumplimiento. En todos estos casos, la situación de incumplimiento debe ser autorizada previamente mediante un proceso de aceptación del riesgo. Este proceso requiere un memo de aceptación de riesgo firmado por el gerente del departamento y autorizado por los departamentos de Seguridad Informática, de Sistemas Informáticos y de Auditoría Interna. Se pueden obtener más detalles acerca del proceso de aceptación de riesgo a través del departamento de Auditoría Interna.

Mayor Información—Las preguntas acerca de este documento deben dirigirse al gerente del departamento de Seguridad Informática. Puede encontrarse información de esta política en el Manual de Recursos Humanos [aquí puede insertarse un enlace en Intranet a dicho documento].



Capítulo 6 MODELO DE POLÍTICA DE SEGURIDAD EN TELETRABAJO Y EQUIPOS MÓVILES

ASUNTOS GERENCIALES

Privilegios de Teletrabajo—El trabajar en casa o en algún sitio alternativo convenido, mejor conocido como teletrabajo, constituye una opción gerencial y no un beneficio complementario general para los empleados. El permiso para teletrabajar es concedido al empleado por el gerente, y antes de dar inicio a un acuerdo de teletrabajo, el gerente tiene que estar convencido que el trabajo se puede hacer eficazmente fuera de sede, que el trabajador posee el carácter y los hábitos de trabajo adecuados y que el sitio alternativo es apropiado para la realización de las tareas encomendadas. Los aspectos del sitio de trabajo incluyen la seguridad física e informática de la propiedad de la Empresa X y un ambiente de baja distracción. La gerencia también debe asegurarse de que el método utilizado para medir el rendimiento del trabajador es realista y está claramente especificado, y que la manera de mantenerse en comunicación con otros trabajadores es la adecuada. Una hoja de trabajo o de control para tomar estas decisiones de autorización se puede conseguir en el Centro de Atención al Usuario [aquí se puede insertar un vínculo desde la intranet a la muestra de una hoja de control].

Re-Evaluación Periódica de los Privilegios—Los privilegios informáticos otorgados a los usuarios, inclusive el privilegio de teletrabajo y el acceso remoto a los sistemas de la Empresa X, deben ser reevaluados por la gerencia cada seis meses. El cumplimiento constante de las políticas descritas en este documento y las políticas relacionadas configuran un factor importante en la toma de decisiones de la gerencia respecto de la continuación de un acuerdo de teletrabajo. Las políticas relacionadas incluyen, sin limitantes, el cumplimiento de los convenios de licencia de software y el informar sobre posibles infecciones de virus del computador. Aquí no se reiteran muchas de las políticas relacionadas, ya que aparecen en otros documentos de la Empresa X [aquí se puede insertar el vínculo desde la intranet a la tabla de contenido de las políticas de seguridad informática]. Este documento se limita a los asuntos de seguridad pertinentes a los teletrabajadores y a los usuarios de equipos móviles de computación.

Inspecciones del Sitio de Trabajo—La Empresa X se reserva el derecho de realizar inspecciones físicas de las oficinas de teletrabajo sin previo aviso. Igualmente, la Empresa X se reserva el derecho de examinar los contenidos de cualquier computador que contenga o pueda contener información interna de la Empresa X, incluyendo los computadores que hayan sido comprados por los empleados, contratistas, consultores, temporales y otros. Adicionalmente, la Empresa X se reserva el derecho de inspeccionar por medios remotos, el contenido y la configuración de los computadores utilizados por los teletrabajadores, a través de herramientas de administración de sistemas remotos.

Consistencia en la Seguridad—La información de la Empresa X debe ser protegida en todo momento, de una manera adecuada y acorde al nivel de confidencialidad y criticidad. Las precauciones descritas en esta política son aplicables sin consideración de los medios de almacenaje en los cuales se encuentre la información, la ubicaciones donde se encuentren, los sistemas utilizados para procesarla, las personas que tengan acceso a ella o los procesos utilizados para manipularla. Esto significa que los trabajadores deben proteger la información de la misma manera, se encuentren en las oficinas de la Empresa X, en una habitación de hotel o en una oficina en casa.

Adiestramiento Obligatorio—Los trabajadores de la Empresa X deben haber cumplido un curso de adiestramiento en sistemas de acceso remoto, y haber aprobado el examen en línea correspondiente, antes de recibir privilegios para el uso de telnet, o cualquier otro sistema de comunicación de acceso remoto a datos de comunicación de la Empresa X [aquí se puede insertar el vínculo de acceso al sitio intranet que permita inscribirse y descargar el curso de adiestramiento computarizado].

Derechos de Propiedad Intelectual—La propiedad Intelectual desarrollada o creada mientras un trabajador atienda los negocios de la Empresa X en cualquier sitio alternativo, se considera propiedad exclusiva de la Empresa X. Tal información intelectual incluye los derechos de patentes, de autor, de marca de fábrica y

todos los otros derechos a propiedad intelectual según se manifieste en memos, planes, estrategias, productos, programas de computación, documentación y otros materiales de la Empresa X.

Participación de Pérdidas o Daños—Los trabajadores que se desempeñen en sitios remotos deben participar con prontitud a su gerente, cualquier daño o pérdida de

hardware propiedad de la Empresa X, así como, software o información confidencial que hayan sido confiados a su cuidado [aquí se puede insertar un vínculo desde la intranet al Sistema de Control y Seguimiento de Casos del Centro de Atención al Usuario].

CONTROL DE ACCESO

Cifrado y Protección de Arranque—Todos los computadores utilizados para teletrabajo, así como los portátiles, laptops, notebooks y otros computadores transportables que contengan información sensible (Confidencial o Secreta) propiedad de la Empresa X, deben utilizar de manera consistente tanto el cifrado en el disco duro de todos los archivos de información, como protección de arranque mediante contraseña. Estos dos controles esenciales deben ser provistos por medio de software o hardware aprobados por el departamento de Seguridad Informática [aquí se puede insertar un vínculo a la lista aprobada de productos de seguridad informática.] Los asistentes digitales personales, los computadores de mano y los teléfonos inteligentes no deben ser utilizados para manejar información sensible de la Empresa X, salvo que estén configurados con los controles necesarios, tales como protectores de arranque y cifrado, ya autorizados para tal uso por el departamento de Seguridad Informática. Se hará excepción con

los calendarios, las libretas de direcciones y la información de conexiones almacenada, tales como los números telefónicos.

Dispositivos de Acceso y Sistemas Compartidos—Los teletrabajadores no deben compartir las tarjetas de contraseñas dinámicas, las tarjetas inteligentes, las contraseñas fijas o cualquier otro dispositivo de acceso o parámetros con persona alguna, sin la aprobación previa del departamento de Seguridad Informática. Esto significa que un computador a distancia utilizado por la Empresa X debe ser utilizado exclusivamente por el teletrabajador. No se debe permitir al círculo familiar, a los amigos o a otras personas la utilización de esta máquina. Los teletrabajadores nunca deben prestar a otras personas el uso de computadores de mano, un asistente digital personal, un teléfono inteligente o cualquier otro computador que almacene información de las actividades de negocios de la Empresa X.

RESPALDO Y ALMACENAMIENTO DE MEDIOS

Respaldo—Los teletrabajadores son responsables de garantizar que sus sistemas remotos sean respaldados periódicamente, bien de manera automática en la red o de manera remota con cintas o equipos similares. Si el respaldo no se puede realizar en la red, la Empresa X debe proporcionar a los teletrabajadores un equipo de respaldo local. Si los respaldos se hacen localmente, los teletrabajadores deben almacenar copias de éstos en un sitio seguro alejado de su sitio de trabajo, por lo menos cada dos semanas. Si los respaldos contienen información confidencial, deben estar cifrados mediante software aprobado por el departamento de Seguridad Informática [aquí se puede insertar un vínculo a la lista de productos de seguridad informática autorizados].

Marcado y Almacenamiento de Medios Confidenciales—Cuando se guarde información confidencial en un disco floppy, cinta magnética, CD-RW u otro medio de almacenamiento, éstos deben ser marcados externa-

mente con la más alta clasificación de confidencialidad correspondiente. Cuando no estén en uso, y a menos que estén cifrados, estos medios deben ser almacenados en un mueble macizo bajo llave. Las tarjetas inteligentes y los módulos de seguridad a prueba de violación constituyen excepciones a esta norma.

Sincronización Automática de Dispositivos—Aquellos sistemas que automáticamente intercambian datos entre dispositivos, tal como el mecanismo de sincronización de archivos utilizado entre un asistente digital personal y un computador personal, no deben estar activados a menos que hayan sido evaluados y autorizados por el departamento de Seguridad Informática.

Fijación de Hora y Fecha—Los teletrabajadores deben ser diligentes en el mantenimiento de la fecha y hora correctas en los relojes internos del computador remoto.

ENLACES DE COMUNICACIONES

Establecimiento de Facilidades de Discado—Los trabajadores no deben dejar sus computadores desatendidos con el modem encendido y el software de comunicaciones activado, a menos que tengan instalado un sistema de control de acceso autorizado por el departamento de Seguridad Informática [aquí se puede insertar un vínculo intranet a la lista de productos autorizados de seguridad informática]. Los trabajadores no deben establecer ningún sistema de comunicaciones que normalmente acepten llamadas entrantes discadas, salvo cuando estos sistemas hayan sido aprobados por el gerente de Seguridad Informática [aquí se puede insertar un vínculo a la Política de Seguridad de Comunicaciones Externas].

Discado Entrante a las Redes de la Empresa X—Todas las líneas entrantes de discado a las redes internas de la Empresa X y a los sistemas computarizados en red deben pasar a través de un punto adicional de control de acceso, tal como un cortafuego, un grupo de conexiones de módem, una interfaz de telecomunicaciones o un sistema similar, antes de permitir a los usuarios acceder a una pantalla de inicio de sesión basada en sistema operativo que solicite un identificador de usuario y una contraseña fija. Este punto adicional de acceso debe emplear contraseñas dinámicas u otra tecnología de autenticación extendida del usuario, aprobada por el departamento de seguridad informática [aquí se puede insertar un vínculo a la lista de productos aprobados por el departamento de Seguridad Informática].

Establecimiento de Conexiones Internet—Los trabajadores no deben instalar cortafuegos, enrutadores, servidores de comunicaciones u otros medios en sus sistemas de computación remotos que manejen negocios de la Empresa X, si dichos medios permiten acceso telnet u otro tipo de acceso entrante en tiempo real a través de Internet. Las conexiones salientes desde un sistema remoto a través de Internet, que desemboquen en un sistema computarizado en red de la Empresa X, serán permitidas siempre que dichas conexiones estén aseguradas por un paquete de software de red privada virtual, según la definición de la Política de Seguridad de Comunicaciones Externas [aquí se puede insertar un vínculo].

Otras Conexiones—Aparte de las conexiones discadas e Internet, los trabajadores no deben instalar ninguna interfase entre un computador remoto utilizado en las actividades de negocios de la Empresa X y cualquier otra red, tales como las redes de valor agregado, salvo

que se haya obtenido la autorización escrita del departamento de Seguridad Informática; lo que significa que los trabajadores tienen prohibido establecer sus propias cuentas personales con proveedores de Internet, para uso en los negocios de la Empresa X. Por lo tanto, todos los negocios por correo electrónico y navegación en internet de la Empresa X se debe realizar a través de un cortafuego administrado por la Empresa X y el software de correo electrónico de la Empresa X [aquí se puede establecer un vínculo a esa parte de la Política de Seguridad de Comunicaciones Externas].

Líneas de Suscripción Digital (DSL) y Líneas de Módem por Cable—Las líneas de suscripción digital, las líneas de modem por cable y otras líneas de alta velocidad no se deben usar por ninguna de las comunicaciones de negocios de la Empresa X, salvo cuando se emplee un cortafuego y una red privada virtual autorizada. Los teletrabajadores deben comunicarse con el Centro de Atención al Usuario para recibir las instrucciones apropiadas para el establecimiento de estas instalaciones antes de llegar a acuerdos con proveedores externos.

Redes de Radio—Los trabajadores que transmitan información sensible de la Empresa X no deben emplear redes de radio, tales como módem de celulares, a menos que dichos canales estén cifrados. El uso de protocolos digitales de comunicación, en lugar de los protocolos analógicos tradicionales de comunicaciones, no se considera cifrado.

Conversaciones Telefónicas—Los trabajadores deben tomar medidas para evitar discutir información confidencial por teléfono. Si el manejo de tal información es absolutamente necesario, los trabajadores deben ejercer cuidado en el uso de términos y evitar la mención de detalles delicados más allá de los necesarios para cumplir con el asunto. La información secreta no debe ser discutida a través de parlantes telefónicos, excepto cuando todas las partes involucradas reconocen que ninguna persona no autorizada se encuentra en los alrededores como para poder escuchar la conversación. La información secreta de la Empresa X nunca se debe tratar a través de teléfonos inalámbricos o celulares, a menos que se use un sistema de cifrado autorizado por el departamento de Seguridad Informática.

Máquinas Contestadoras—Los trabajadores deben abstenerse de dejar información confidencial en estos sistemas reproductores de voz, a menos que las máquinas contestadoras o sistemas de correo de voz

estén protegidos con contraseña. Los teletrabajadores deben grabar un mensaje saliente en el cual informen a los interlocutores que el sistema de mensajes entrantes no está dotado de seguridad y que no es apto para recibir

información confidencial, excepto cuando las máquinas contestadoras o sistemas de voz estén protegidos con contraseña.

ADMINISTRACIÓN DEL SISTEMA

Máquinas Suministradas por la Empresa X—Los empleados que trabajan en los negocios de la Empresa X en sitios alternativos deben usar equipos de red y de computación suministrados por la Empresa X. Se hará excepción sólo cuando otros equipos hayan sido autorizados por el Centro de Atención al Usuario por su compatibilidad con los controles y sistemas informáticos de la Empresa X.

Sistema de Control de Acceso—Los teletrabajadores no deben utilizar ningún computador remoto en las actividades de negocios de la Empresa X, que no ejecute un sistema de control de acceso aprobado por el departamento de Seguridad Informática [aquí se puede insertar un vínculo a la lista de productos autorizados].

Sistemas de Teletrabajo—Los trabajadores encargados de los negocios de la Empresa X en sitios de trabajo alternativos deben usar únicamente el software, hardware y equipos de redes de computadores suministrados por la Empresa X. Se hará excepción sólo cuando otros equipos hayan sido aprobados por el departamento de Seguridad Informática por su compatibilidad con los sistemas y controles de la Empresa X. Los trabajadores no deben llevar computadores de su propiedad a las oficinas de la Empresa X para procesar, o de manera alguna manejar, información sin la previa autorización del departamento de Sistemas Informáticos.

Cambios en Configuración y Software—En el hardware de computación suministrado por la Empresa X, los trabajadores no deben hacer cambios en la configuración del sistema operativo o instalar software nuevo. Si se requieren tales cambios, éstos deben ser realizados por el personal del Centro de Atención al Usuario a través del software de mantenimiento de sistemas remotos. Cambiar la fuente tipográfica predeterminada de un programa de procesador de palabras, o de alguna manera cambiar las plantillas suministradas por una aplicación, se permite sin la asistencia del Centro de Atención al Usuario y sin autorización previa.

Cambios en el Hardware—El equipo de computación suministrado por la Empresa X no debe ser alterado de manera alguna, sin previo conocimiento y autorización del Centro de Atención al Usuario.

Descarga de Software—Los trabajadores no deben descargar software de foros electrónicos, de Internet o de otro sistema externo a la Empresa X, a los computadores utilizados para el manejo de datos de la Empresa X.

Propiedad Versus Posesión—Si la Empresa X suministra a un teletrabajador software, muebles, información u otros materiales para conducir los negocios de la Empresa X remotamente, el título de propiedad y todos los derechos e intereses sobre dichos artículos permanecerán con la Empresa X. En tales casos, la posesión por el teletrabajador no significa traspaso de propiedad o ninguna insinuación de que sea su propiedad. Todos los artículos deben ser devueltos a la Empresa X cuando un teletrabajador se separe de la Empresa X, o cuando así lo solicite el gerente del teletrabajador.

Responsabilidad por la Propiedad de la Empresa X—Si la Empresa X suministra al teletrabajador software, hardware, muebles, información u otros materiales para realizar las actividades de negocio correspondientes, la Empresa X asumirá todo el riesgo de pérdida o daño a dichos artículos, salvo cuando tal pérdida o daño sea ocasionado por negligencia del teletrabajador. La Empresa X deniega expresamente cualquier responsabilidad por pérdida o daño a terceros o su propiedad, causada por tales artículos o que surja del uso de los mismos.

Interferencia Electromagnética—En algunos casos, el uso de computadores u otros dispositivos electrónicos genera interferencia electromagnética que afecta televisores, radios, u otras máquinas. Si alguna instalación del sistema de teletrabajo para realizar negocios de la Empresa X genera tal interferencia, su uso debe terminar de inmediato mientras se identifica la naturaleza del problema y su solución. El Centro de Atención al Usuario de la Empresa X ayudará a los teletrabajadores durante este proceso [aquí se puede insertar un vínculo a la página de intranet del Centro de Atención al Usuario].

CONSIDERACIONES EN TRASLADOS

Retiro de Información—La información sensible (Confidencial o Secreta) no puede ser removida de la Empresa X, salvo cuando el Propietario de la información lo haya autorizado previamente. Esta política incluye información sensible almacenada en discos duros de computadores, en discos flexibles, CD-ROM, cartuchos de cintas magnéticas y memos en papel, con excepción de los respaldos autorizados fuera de sede que estén cifrados [aquí se puede insertar un vínculo a la Política de Clasificación de la Información].

Viajes con Información Secreta—Los trabajadores deben evitar los viajes en transporte público cuando tengan en su posesión información secreta de la Empresa X, a menos que un gerente local de departamento lo haya autorizado específicamente.

Traslado al Extranjero—Cuando un trabajador traslade información Secreta de la Empresa X al extranjero, la información debe estar almacenada de alguna manera inaccesible, tal como un disco flexible cifrado, o debe estar en posesión del trabajador en todo momento. Los trabajadores de la Empresa X no deben llevar información Secreta de la Empresa X a otro país, a menos que cuenten con la autorización de la gerencia de Seguridad Física.

Exposición Pública—La información confidencial de la Empresa X no debe ser leída, discutida o de manera alguna expuesta en restaurantes, en aviones, en trenes o en cualquier lugar público donde puedan descubrirla personas no autorizadas.

Chequeo de Equipaje—Los trabajadores que transporten consigo equipos portátiles, laptops, notebooks, palmtops, manuales, teléfonos inteligentes, asistentes digitales personales y otros computadores transportables que contengan información sensible, no deben entregar dichos computadores a los sistemas de equipaje de las aerolíneas, sino que deben llevarlos consigo como equipaje de mano.

Aseguramiento de Información Confidencial en Papel—Cada vez que se retire de las sedes de la Empresa X alguna información Secreta en papel, ésta debe ser almacenada en un mobiliario seguro y con cerradura, o en algún contenedor pesado con cerradura, o transportado en un maletín con cerradura cuando no esté en uso. Tal información no se puede dejar desatendida en un vehículo, cuarto de hotel u oficina externa, aunque estén bajo llave.

Envío Vía Fax de Información Confidencial—Si se envía información Secreta por fax, el destinatario debe haber sido notificado de la hora en que será transmitida, y también debe haber acordado que una persona autorizada esté presente en la máquina de destino en el momento de la transmisión. Se puede hacer una excepción cuando el área de la máquina de fax se encuentra restringido de tal manera que no puedan ingresar personas no autorizadas para leer dicho material. Esto significa que la información confidencial de la Empresa X no debe ser enviada por fax a través de una recepción de hotel o de terceras partes que no sean confiables. Otra excepción se hará en aquellas instancias en las cuales las máquinas de fax de destino estén protegidas por contraseñas, a las cuales sólo tengan acceso personas autorizadas.

SEGURIDAD FÍSICA

Similitud en el Enfoque—Se deben tomar precauciones razonables en los sitios de trabajo alternativos, para proteger el hardware, el software y la información propiedad de la Empresa X contra hurtos, daños y abusos.

Suministro de Contenedores Seguros—Los trabajadores que deban mantener información Secreta o Confidencial en sus casas de la Empresa X, deben poseer caja fuerte o mobiliario pesado con cerradura para guardar adecuadamente tal información. Si no poseen el mobiliario o caja fuerte, la Empresa X debe proporcionarlos en préstamo.

Trituradoras—Los teletrabajadores deben tener o se les debe suministrar, trituradoras para desechar de manera apropiada las versiones impresas de la información confidencial. Las trituradoras que hacen tiras de papel no son aceptables para la eliminación de material confidencial de la Empresa X. Las unidades aceptables son aquéllas que convierten el papel en confeti u otras partículas pequeñas. Toda la información confidencial en papel, además de cualquier información que contenga números de cuentas financieras, como los de las tarjetas de crédito, deben ser trituradas. Los productos intermedios del trabajo que contengan información confidencial, tales como copias de papel

carbón, fotocopias, negativos fotográficos o borradores de memos en papel, también deben triturarse. Los teletrabajadores en viajes no deben desechar información confidencial de la Empresa X en las cestas de basura de los hoteles o en otros contenedores públicos de basura. La información confidencial se debe resguardar hasta que sea triturada o destruida con otros métodos autorizados.

Pases de Propiedad—Los computadores portátiles, teléfonos celulares, asistentes digitales personales, módems y otros equipos de sistemas informáticos relacionados propiedad de la Empresa X, no deben salir de las oficinas de la Empresa X si no van acompañados con pase de propiedad. Deben obtenerse pases de propiedad al traer equipos personales a las oficinas de la Empresa X. El equipo de computación propiedad de la Empresa X que esté situado en un sitio de trabajo remoto, no debe ser trasladado a otro sitio sin la previa autorización del gerente del teletrabajador. Se exceptuarán aquellos equipos con su respectivo pase de propiedad autorizado.

Traslado de Residencia—Si un teletrabajador tiene la intención de mudarse de residencia, o mudarse de un

sitio de trabajo a otro, el trabajador debe notificar a su gerente y conseguir la previa autorización correspondiente. El trabajador también debe seguir las instrucciones del departamento de Seguridad pertinentes a la mudanza de residencia del teletrabajador. La nueva residencia debe reunir todos los requisitos vigentes para ser sede de teletrabajo [aquí se puede insertar un vínculo a la lista de verificación de los teletrabajadores].

Posicionamiento de la Pantalla—Las pantallas correspondientes a cualquier sistema utilizado para manejar la información confidencial de la Empresa X, deben ser posicionadas de manera que no puedan ser fácilmente visualizadas por personas no autorizadas a través de ventanas, por encima del hombro o maneras similares.

Cierre de Sesión—Después de completar su sesión remota con los computadores de la Empresa X, el trabajador debe cerrar la sesión y luego colgar, en lugar de sólo colgar. Los trabajadores que utilicen comunicaciones remotas deben esperar la señal de confirmación de su comando de cierre de sesión de parte de la máquina remota de la Empresa X, antes de alejarse de su computador.



Capítulo 7 MODELO DE POLÍTICA DE SEGURIDAD EN COMUNICACIONES EXTERNAS

Objetivos y Alcance de la Política—Esta política describe los requerimientos de seguridad para las conexiones de los sistemas de información remotos a las computadoras internas y redes de la Compañía X y cubre una amplia variedad de tecnologías que incluye conexiones de teléfonos celulares, enlaces de modem de discado, redes con valor agregado y redes con valor agregado de Internet. Cada trabajador individual u organización que realice éstos y otros tipos de conexiones remotas automatizadas a las computadoras y redes de la Compañía X deberá seguir las reglas aquí descritas.

Conexiones Externas Requieren de Autorización—En todos los casos, el acceso a las redes internas de la Compañía X desde lugares remotos, tales como los hogares de los trabajadores, las habitaciones de hoteles y las oficinas de servicios al cliente, deberá estar previamente autorizado por el gerente inmediato del trabajador involucrado. Dicho acceso remoto no es un beneficio extra y podrá ser revocado en cualquier momento por causas que incluyen un desempeño deficiente y el incumplimiento de las políticas de seguridad. Dentro de la Política de Seguridad de Teletrabajo se pueden encontrar detalles adicionales acerca de este proceso de autorización [insertar un enlace al sitio de intranet en donde existe este documento].

Acceso de Terceros a las Redes Internas de la Compañía—En situaciones estrictamente controladas, la Empresa X permite el acceso de terceros a las redes internas y a los sistemas conectados de las computadoras de la Empresa X. El Propietario de la información a la cual el tercero tendrá acceso y el gerente del proyecto responsable del trabajo del tercero deberán acordar por escrito cómo se efectuará dicho acceso antes de que éste se establezca. El proceso de toma de decisiones para otorgar el acceso incluye la consideración de los controles en los sistemas a ser conectados, de las políticas de seguridad del tercero, de si se ha suscrito un acuerdo de confidencialidad y de los resultados de una verificación de antecedentes. Los privilegios del sistema para terceros deberán limitarse estrictamente a los servicios del sistema y a la información necesaria para lograr los objetivos

predefinidos del negocio. El gerente principal del proyecto deberá revisar estos privilegios de acceso cada seis meses para determinar si es necesario mantenerlos.

Acceso de Proveedores Terceros—A los Proveedores Terceros que hayan vendido a la Empresa X, bien sea hardware, software o servicios de comunicación, no se otorgará en forma automática el acceso repetido a las computadoras y redes internas de la Empresa X. Para el proceso de mantenimiento de los sistemas que el departamento de Seguridad Informática administra, ellos deberán pasar a través del proceso de autorización descrito en el párrafo anterior o a través de un acceso remoto separado [insertar un enlace intranet para obtener información sobre el departamento respectivo]. Un administrador del sistema podrá habilitar privilegios de acceso remoto temporal para los proveedores, obviando cualquiera de estos procesos. Sin embargo, este acceso temporal se otorgará únicamente por el periodo de tiempo que sea necesario para completar las tareas autorizadas, de un día o menos. Este acceso temporal proveerá al personal del proveedor una identificación positiva antes de que se establezca la conexión y llevará el registro de toda la actividad realizada mientras exista la conexión.

Declaración de Cumplimiento por Parte de Terceros—Todos los terceros que deseen acceder en forma remota a las computadoras y redes internas de la Empresa X deberán firmar una declaración de cumplimiento antes de que se les otorgue un código de identificador de usuario. Si algún tercero ya posee este código, deberá obtener una firma antes de recibir la renovación del mismo, la cual se realiza cada seis meses. La firma de esta declaración de cumplimiento indica que el usuario entiende y acuerda cumplir las políticas y procedimientos de la Empresa X en relación con las computadoras y las redes. La Empresa X se reserva el derecho de auditar de manera periódica a los terceros que tengan acceso a las computadoras y redes de la Empresa X para asegurar que se cumplen ésta y otras políticas y requerimientos.

Responsabilidad por los Identificadores de Usuario—Todos los trabajadores, incluyendo los de terceros, son responsables de las actividades que realicen con su identificador de usuario, aunque estos códigos se conecten a través de instalaciones de redes

externas, y nunca se deberán compartir con compañeros de trabajo, amigos, familiares u otras personas. Tampoco deberán ser utilizados por ninguna persona distinta a aquella a quien se le otorgó. Igualmente, se prohíbe a los trabajadores realizar cualquier actividad con aquellas identificaciones de usuario que pertenezcan a otras personas con la excepción de aquellos identificadores de usuario anónimo, como por ejemplo "visitante".

Denegación por Defecto—Si el computador o el sistema de control de acceso a la red de la Empresa X no está funcionando adecuadamente, deberá por defecto denegar los privilegios a los usuarios. Cuando los sistemas de control de acceso fallan, los sistemas que ellos soportan no podrán estar disponibles hasta tanto el problema se haya solucionado.

Contraseñas Dinámicas—Todas las conexiones de red que se inicien desde una ubicación fuera de una sede oficial de la Empresa X y que se conecten a una red interna de la Empresa X, deben emplear sistemas de contraseñas dinámicas autorizados por el departamento de Seguridad Informática. Las contraseñas dinámicas son aquellas que se modifican cada vez que se establece una nueva sesión y no se requieren para las conexiones de red tipo 'almacenar y enviar', tales como las que se emplean para el correo electrónico y los servicios de noticias de Internet.

Conexiones Salientes—Las conexiones de red de computadores que se inicien desde una sede oficial de la Empresa X y que se conecten a un computador o a una red externa no requieren del uso de contraseñas dinámicas. Dichas conexiones se deben enrutar a través de grupos de módems de discado, cortafuegos de Internet y otros sistemas establecidos expresamente para proveer un acceso seguro a la red.

Módem en Sistemas de Escritorio—No se permitirá el uso de módems dentro de las oficinas de la Empresa X o que estén conectados a los computadores personales (PC) de escritorio de las oficinas, exceptuando los PC de uso doméstico, portátiles o de teletrabajo. Las conexiones a computadores y redes remotas se deben encaminar a través de los grupos de módems o el cortafuego de Internet de la Empresa X. Por consiguiente, salvo que se instale un sistema de contraseña dinámica, los trabajadores que posean PC de uso doméstico, portátiles o de teletrabajo, no deben dejar los módems en el modo contestación automática con el software de comunicaciones activado de manera que se puedan recibir las llamadas discadas.

Enlaces Cifrados—Cada vez que se establece una conexión de red entre un computador de la Empresa X y otra ubicada fuera de una sede oficial de la Empresa X y cada vez que esta conexión transmita o pueda transmitir información Confidencial o Secreta, el enlace se debe cifrar. Dicho cifrado se debe realizar únicamente con sistemas autorizados por el departamento de Seguridad Informática [Insertar un enlace intranet a la lista de productos autorizados emitida por el departamento de Seguridad Informática]. Estos sistemas incluyen redes privadas virtuales que incorporan no sólo el cifrado sino también los mecanismos para la autenticación de los usuarios.

Empleo de Tecnología de Radio para Datos—Los teléfonos portátiles y celulares que emplean tecnología de radio no se deben usar para las transmisiones de datos que contengan información Confidencial o Secreta de la Empresa X, salvo que la conexión esté cifrada. Otras tecnologías de red de transmisión tales como las redes de área local basados en tecnología de radio no se deben emplear para esta clase de información de la Empresa X a menos que el enlace esté cifrado. Dichos enlaces pueden utilizarse para el correo electrónico, siempre y cuando los usuarios entiendan que las transmisiones no deben contener información Confidencial o Secreta que pueda ser leída. Los trabajadores tampoco deben discutir asuntos Confidenciales o Secretos por teléfonos inalámbricos o celulares que empleen una conexión normal de voz, salvo que haya sido cifrada con una tecnología autorizada por el departamento de Seguridad Informática (insertar un enlace intranet a la lista de productos autorizados). Igualmente, los teléfonos que utilicen protocolos de transmisión digital en lugar de protocolos de transmisión analógica no se considerarán cifrados para los efectos de esta política.

Controles de Acceso Privilegiado—Todos los computadores que estén conectados de manera permanente o intermitente, bien sea a redes externas o a redes de la Empresa X, deben operar con controles de acceso privilegiado autorizados por el departamento de Seguridad Informática [insertar un enlace intranet a la lista de productos autorizados]. Los sistemas multiusuario deben emplear identificadores de usuarios exclusivos para cada usuario y mecanismos de restricción de privilegios a usuarios que incluyen permisos de acceso al directorio y a los archivos, mientras que los sistemas para un solo usuario conectados a las redes deben emplear mecanismos autorizados de hardware o software que controlen el sistema de inicio y que incluyan un protector de pantalla con mecanismo de desconexión después de cierta inactividad.

Cambio de Contraseñas Iniciales—Todas las contraseñas predeterminadas suministradas por el proveedor, así como otros mecanismos alternativos de acceso, deben cambiarse antes de que la Empresa X emplee un computador o un sistema de comunicación para sus actividades de negocio. Esta política se aplica a contraseñas asociadas con identificadores de usuario, a contraseñas asociadas a administradores de sistemas y otros identificadores de usuario privilegiado.

Sistemas de Archivos Compartidos—El establecimiento de una conexión entre un computador o una red externa y un computador o una red interna de la Empresa X no debe incluir el uso de sistemas de archivos compartidos, exceptuando aquellos casos en los que el departamento de Seguridad Informática autorice la configuración antes de su uso.

Requerimiento de Programas Antivirus—Los programas antivirus autorizados por el departamento de Seguridad Informática [insertar un enlace intranet en la lista de productos autorizados] se habilitarán de manera continua en todos los servidores web, servidores de correo, cortafuegos y computadores personales en red, exceptuando aquellos casos en donde el sistema operativo no esté susceptible de virus.

Erradicación de Virus—Los trabajadores no deben intentar erradicar los virus sin contar con ayuda experta. Cuando se sospeche de una infección por virus o cuando el software antivirus señale que existe una infección, los trabajadores deben dejar de usar el computador de inmediato, desconectar en forma física el equipo de todas las redes y llamar al Centro de Atención al Usuario (insertar su número de teléfono o un enlace a su página intranet). En caso de que el virus sospechoso pareciera estar ocasionando daños en la información o en el software, se debe apagar el computador de inmediato.

Descompresión antes de Ejecutar el Software Antivirus—Todos los archivos provenientes de fuentes externas y que puedan ser leídos por el computador se deben descomprimir antes de someterlos a un proceso autorizado antivirus. Esto se aplica a archivos cifrados.

Sistemas sin Parches o Infectados con Virus—Se debe desconectar de la red de la Empresa X a aquellos trabajadores que no hayan instalado los parches requeridos en el software de sus computadores remotos o cuyos sistemas estén infectados por virus, hasta que se haya restaurado un ambiente informático seguro. Con el objeto de verificar con regularidad el estatus de los sistemas conectados en forma remota, la Empresa X debe emplear un software de administración remota que

examine los archivos almacenados, las configuraciones del sistema y el software instalado. Los trabajadores que se conecten con la red de la Empresa X deben estar de acuerdo con dicho monitoreo remoto.

Descarga de Software—Los trabajadores no deben descargar software desde sistemas de foros y boletines electrónicos, Internet y otros sistemas ubicados fuera de la Empresa X, con excepción de los administradores de sistemas y otro personal técnico autorizados para bajar parches y paquetes de software actualizados. De igual manera, se contemplan excepciones para los sistemas automatizados de distribución de software para redes externas como aquellos que distribuyen el software antivirus más reciente y que hayan sido autorizados por el departamento de Seguridad Informática [insertar un enlace intranet a la lista de productos autorizados emitida por el departamento de Seguridad Informática].

Descarga de Contenido y Asignación de Etiquetas—Con las únicas excepciones de la correspondencia comercial general y el software con derechos reservados, toda la información proveniente de fuentes externas que no sea claramente de dominio público debe recibir una etiqueta del sistema de clasificación de la información de la Empresa X. El trabajador de la Empresa X que reciba esta información tendrá la responsabilidad de asignar una etiqueta de clasificación apropiada en representación del tercero. Al realizar la asignación, el trabajador debe guardar los avisos de derechos reservados, los créditos a autores, los lineamientos de interpretación y las restricciones para su divulgación. En la Política del Sistema de Clasificación de Datos, se podrán encontrar detalles adicionales [insertar un enlace de intranet a dicho documento].

Confiabilidad del Contenido Descargado—Toda la información proveniente de la Internet y otras redes externas debe considerarse no confiable hasta confirmarla a través de otras fuentes.

Mecanismo de Desconexión después de Cierta Inactividad—Todos los sistemas de información que acepten conexiones remotas desde redes públicas tales como la red telefónica discada o la Internet deben incluir un mecanismo de desconexión, el cual finalizará todas las sesiones que permanezcan inactivas por un periodo de 30 minutos o menos. Todos los identificadores de usuario registrados en redes o computadores con servicios de acceso externo deben suspenderse en forma automática luego de 30 días de inactividad.

Incapacidad de Establecer una Conexión—Todos los computadores de la Empresa X con interfaces a redes externas deben finalizar temporalmente la conexión o

utilizar un tiempo muerto para el identificador del usuario de por lo menos 10 minutos después de una secuencia de intentos fallidos por entrar al sistema. Estos intentos fallidos repetidos para establecer una conexión empleando un identificador de usuario privilegiado no deben tener como consecuencia su revocación.

Avisos de Prohibición de Entrada sin Autorización—En aquellos casos en los que el software de sistemas lo permita, se deben emplear mensajes al inicio de sesión en todas las redes y computadores de la Empresa X directamente accesibles a través de redes externas. Estos mensajes deben emplear los avisos normales de prohibición de entrada establecidos por el departamento de Seguridad Informática, los cuales además se deben abstener de revelar que se han conectado a los sistemas de la Empresa X, la naturaleza de la información disponible en los mismos y el software de sistemas específico que se ejecuta en estos computadores. Los servidores web, las unidades de teléfono de respuesta de voz y otros sistemas diseñados para responder a usuarios anónimos no necesitan disponer de tales avisos.

Interacción Anónima—Con las únicas excepciones de los servidores web, los foros y boletines electrónicos y otros sistemas en donde todos los usuarios regulares son anónimos, los usuarios no se deben conectar al sistema o a la red de la Empresa X en forma anónima. Si los usuarios emplean servicios del sistema que les permitan cambiar su identificador de usuario para obtener ciertos privilegios, deberán haberse conectado inicialmente empleando un identificador de usuario que claramente indique su identidad.

Registros para Sistemas Conectados Externamente—Todos los computadores y las redes de la Empresa X que hacen interfase con redes externas deben guardar registros que indiquen la identidad y la actividad realizada por cada usuario que accede a estos sistemas. Dichos registros deben indicar la hora del día, la fecha, el identificador de usuario empleado, cualquier privilegio utilizado y otros detalles relacionados con todas las conexiones. Los administradores del sistema deben revisar los resúmenes de estos registros y emplear sistemas automatizados de detección de intrusos, autorizados por el departamento de Seguridad Informática, para informarles de inmediato de cualquier actividad sospechosa [insertar un enlace a la página intranet con la lista de productos autorizados de seguridad informática].

Control de Flujo para Sistemas Conectados Externamente—Todas las redes de la Empresa X que estén conectadas a redes externas deben emplear mecanismos

de control de flujo para restringir las máquinas a las cuales los usuarios se puedan conectar con base en la necesidad que existe para tal acceso. Dicho control se puede llevar a cabo a través de cortafuegos internos, enruteadores, puertas de enlace, interfaces y otros componentes de la red.

Exploración—Con la excepción de la intranet de la Empresa X, los trabajadores no deben explorar los sistemas y las redes de la Empresa X. Por ejemplo, queda prohibida la búsqueda, por curiosidad, de archivos y programas interesantes en los directorios de otros usuarios. Las gestiones que el trabajador realice para encontrar en forma legítima la información necesaria para llevar a cabo su trabajo no se considera exploración. Esta declaración acerca de la exploración no se aplica a redes externas como la Internet.

Obtención de Acceso No Autorizado—Los trabajadores que utilicen las redes de computadores de la Empresa X no deben acceder sin autorización a ningún sistema de información o red a los cuales no se les haya otorgado expresamente el acceso; de igual manera, queda prohibido dañar, interrumpir o interferir en las operaciones de los sistemas de información multiusuario a los cuales están conectados. Los trabajadores no deben capturar o de algún otro modo poseer contraseñas, claves de cifrado o cualquier otro mecanismo de control de acceso que no les haya asignado expresamente, ni tampoco pueden poseer o utilizar herramientas de software que pudiera permitir el acceso no autorizado a los recursos del sistema.

Modificaciones a las Redes de la Empresa X—Las modificaciones a las redes internas de la Empresa X incluyen la instalación de software nuevo, el cambio de las direcciones de las redes, la reconfiguración de enruteadores y el agregado de líneas de discado. Exceptuando los casos de emergencia, todas las modificaciones a las redes de computadores de la Empresa X se deben documentar en una solicitud de orden de trabajo [insertar aquí un enlace intranet a dicho formulario] y deben estar autorizadas con anterioridad por el departamento de Tecnología Informática. Las modificaciones de emergencia que se realicen a las redes de la Empresa X deben ser llevadas a cabo únicamente por personas que estén autorizadas por el departamento de Tecnología Informática.

Establecimiento de Conexiones al Sistema—Los trabajadores no deben instalar o hacer arreglos para la instalación de sistemas de foros y boletines electrónicos, redes de área local, conexiones de modem a redes de área local existentes u otros sistemas multiusuarios para transmitir información sin la autorización específica del

director del departamento de Tecnología de Información. No se deben establecer nuevos tipos de conexiones en tiempo real entre dos o más sistemas de computación internos a menos que se haya obtenido dicha autorización.

Instalación de Líneas de Comunicaciones—Los trabajadores y los proveedores no deben hacer arreglos ni completar la instalación de líneas de datos o de voz con ningún proveedor sin la autorización del director del departamento de Sistemas Informáticos [insertar un enlace intranet a un formulario con este fin].

Suscripción a Redes Externas—Los trabajadores no deben establecer conexiones con proveedores de Internet (ISP, en inglés) u otras redes externas para la transmisión de datos de la Empresa X, a menos que el director del departamento de Seguridad Informática haya autorizado este convenio. Para obtener información adicional sobre los ISP, ver la Política de Seguridad de Internet [Insertar aquí un enlace de intranet].

Establecimiento de Nuevas Redes de Negocios—A menos que el director de Tecnología Informática y el principal asesor legal otorguen la autorización, los trabajadores no deben usar la Internet o cualquier otra red externa para establecer nuevos o diferentes canales de negocio. Estos canales incluyen acuerdos para el intercambio de datos electrónicos, servicios de base de datos en línea y aceptación de tarjetas de crédito a través de Internet.

Participación en Redes Externas—Queda expresamente prohibida la participación en redes externas como proveedor de servicios a terceros, a menos que el principal asesor legal de la Empresa X haya identificado los riesgos legales que ello implica y el director de Tecnología Informática haya aceptado expresamente estos y otros riesgos relacionados con la propuesta.

Confidencialidad de la Información de los Sistemas—Las direcciones internas, las configuraciones y la información relacionada con el diseño del sistema de redes y computadores de la Empresa X representan información confidencial que no debe divulgarse a terceros quienes no tienen necesidad demostrable de conocer tal información. Las medidas de seguridad que se empleen para proteger las redes y los computadores de la Empresa X son confidenciales y se deben proteger de igual forma.

Información Relacionada—Para obtener información adicional acerca de un tema relacionado, ver la Política de Seguridad de Teletrabajo [insertar aquí un enlace intranet] y la Política de Divulgación de Información de Terceros [insertar aquí un enlace intranet].

Aprobado por : [insertar nombre de ejecutivo]

Aprobado el: DD/MM/AA

Fecha de Vigencia: DD/MM/AA

Número de Versión: XX



Capítulo 8 MODELO DE POLÍTICA DE SEGURIDAD DE COMPUTADORES PERSONALES

BOSQUEJO DEL DOCUMENTO

Objetivos y Alcance—Una buena parte de los negocios de la Empresa X se realiza con computadores personales, incluyendo computadores Macintosh, estaciones de trabajo UNIX, computadores portátiles, computadores de mano, asistentes personales digitales y otros equipos similares dedicados a la actividad de un solo usuario. En la Empresa X, la protección de los computadores personales y la información que manejan es un elemento esencial en los negocios. Es por eso que, con ese objeto, esta política proporciona instrucciones sobre seguridad informática que se aplican a todos los trabajadores que

utilizan los computadores personales de la Empresa X. Se espera que todos los usuarios de estos equipos cumplan con esta política como condición para mantener su empleo, la cual se aplica para los computadores personales independientes y para los que están conectados a redes, tales como la red de área local o la intranet. Para obtener información relacionada, ver Capítulo 6, “[Modelo de Política de Seguridad en Teletrabajo y Equipos Móviles](#)” y Capítulo 12, “[Modelo de Política de Seguridad en Intranets](#).”

SÓLO PARA USO EMPRESARIAL

Sólo para Uso Empresarial—En líneas generales, los sistemas de comunicación y de computadores de la Empresa X están destinados únicamente para usos empresariales; sin embargo, el uso personal adicional está permitido siempre y cuando no consuma una cantidad significativa de recursos que pudieran de otro modo emplearse para propósitos empresariales, no interfiera con la productividad del trabajador, no ocupe un lugar preferente sobre otras actividades del negocio y no ocasione dificultades ni problemas legales o morales

para otros trabajadores. El uso adicional lícito de un computador personal abarcaría, por ejemplo, responder a un mensaje de correo electrónico sobre un almuerzo, comprar un regalo en línea y pagar las cuentas a través de la Internet. Quedan estrictamente prohibidos, en todos los computadores personales de la Empresa X, los materiales ofensivos que pudieran perjudicar su imagen, incluyendo aquéllos cuyo contenido sea sexista, racista, violento u otros.

CONTROL DE LA CONFIGURACIÓN

Modificaciones al Software de las Aplicaciones—La Empresa X tiene una lista de paquetes de software aceptables que los usuarios pueden ejecutar en sus computadores personales [aquí se puede suministrar un enlace a una norma de configuración de computadores personales publicado en la intranet]. Los trabajadores no deben instalar otros paquetes de software en los computadores personales si no obtienen con antelación un permiso del grupo de Computadores Personales del departamento de Sistemas Informáticos. Tampoco deben permitir que se ejecuten rutinas automáticas de instalación de software en los computadores personales de la Empresa X, a menos que hayan sido autorizadas por el mismo grupo. Salvo el caso en que se realicen arreglos por separado con el grupo de Computadores

Personales, las actualizaciones al software autorizado se descargarán en forma automática en los computadores personales, mientras que el software no autorizado podrá ser removido del equipo del trabajador involucrado sin previo aviso.

Modificaciones a las Configuraciones del Sistema Operativo—En el hardware del computador proporcionado por la Empresa X, los trabajadores no deben modificar las configuraciones del sistema operativo, actualizar los sistemas operativos existentes o instalar nuevos sistemas operativos. De requerirse dichos cambios, los mismos deben ser realizados por personal del Centro de Atención al Usuario, en persona o mediante el uso de software de mantenimiento de sistemas remotos.

Modificaciones del Hardware—Los equipos de computación proporcionados por la Empresa X no deben alterarse o modificarse, de ninguna manera, sin el

conocimiento previo o la autorización del grupo de Computadores Personales del departamento de Sistemas Informáticos.

CONTROL DE ACCESO

Paquete de Control de Acceso—Todos los computadores personales de la Empresa X deben ejecutar un paquete de control de acceso autorizado por el departamento de Seguridad Informática [aquí se puede insertar un enlace a la lista de productos autorizados]. Por lo general, estos paquetes requieren de una contraseña fija para el momento en que se inicia un computador personal y nuevamente después de cierto periodo de inactividad. Los usuarios deben fijar el lapso de tiempo para ese periodo de inactividad en 15 minutos o menos, el cual una vez transcurrido obscurece el contenido de la pantalla. Si un computador personal contiene información confidencial, la pantalla se debe proteger de inmediato con este paquete de control de acceso o apagar el equipo cada vez que un trabajador se ausente del lugar en donde el computador personal se encuentra en uso.

Selección de Contraseñas—Las contraseñas elegidas por el usuario y empleadas por los paquetes de software de control de acceso, y las claves empleadas por los paquetes de cifrado, deben tener por lo menos 10 caracteres, los cuales deben ser difíciles de adivinar. No se deben emplear palabras del diccionario, derivaciones de los identificadores de usuario y secuencias de caracteres comunes, como por ejemplo, "123456". Los datos personales tales como el nombre del cónyuge, el número de placa del automóvil, el número de seguro social y la fecha de cumpleaños tampoco se deben usar, salvo que estén acompañados por caracteres adicionales no relacionados. Las contraseñas y las claves elegidas

por el usuario no deben ser partes gramaticales que incluyan nombres propios, ubicaciones geográficas, siglas comunes o jerga.

Almacenamiento de Contraseñas—Los trabajadores deben mantener un control exclusivo de sus contraseñas personales y no deben, en ningún momento, compartirlas con otras personas. Las contraseñas no se deben guardar en formato legible, en comandos automáticos de entrada, en macros, en teclas de función, en computadores sin controles de acceso o en alguna otra ubicación en donde las personas no autorizadas podrían descubrirlas.

Cifrado de Información Secreta—Toda la información confidencial que esté computarizada debe cifrarse cuando no se encuentre en uso activo; por ejemplo, cuando no la esté utilizando un software o no la esté viendo un usuario autorizado. Asimismo, se recomienda el empleo de medidas físicas de seguridad, tales como cajas fuertes, y el cierre del mobiliario y de las puertas de la oficina con llave como medidas adicionales para proteger la información secreta.

Registro de Eventos Relacionados con Información Secreta—Los computadores personales que manejen información secreta deben registrar de manera segura todos los eventos relevantes relacionados con la seguridad del computador. Algunos de estos eventos son: intentos para descifrar la contraseña o para usar privilegios que no hayan sido autorizados, modificaciones al software de las aplicaciones de producción y cambios en el software del sistema.

VIRUS

Programa Antivirus Instalado—Todos los computadores personales deben ejecutar continuamente la versión actual del paquete antivirus autorizado por el departamento de Seguridad Informática [aquí se puede insertar un enlace a la lista de productos autorizados]. La versión actual de este paquete antivirus se debe descargar en forma automática a cada computador personal cuando el equipo se conecte a la red interna de la Compañía X. Los trabajadores no deben abortar este

proceso de descarga. Como mínimo, este paquete se debe ejecutar cada vez que se proporcionen medios externos de almacenamiento.

Descompresión Antes de la Verificación—No deben usarse discos flexibles, CD-ROM u otros medios de almacenamiento removibles suministrados por una fuente externa, a menos que hayan sido verificados con software antivirus. De igual forma, los archivos anexos al correo electrónico no deben ejecutarse o abrirse a menos que hayan sido verificados con software

antivirus. Los archivos que puedan ser leídos por el computador, los programas de software, las bases de datos, los documentos de procesadores de palabras y las hojas de cálculo provenientes de fuentes externas deben descomprimirse antes de someterlos a un proceso antivirus autorizado. Si los archivos han sido cifrados, tienen que ser descifrados antes de ejecutar el software antivirus.

Erradicación de Virus—Los trabajadores no deben intentar eliminar los virus sin contar con ayuda experta. Cuando se sospeche de una infección o cuando el software antivirus señale que existe una infección, los trabajadores deben dejar de usar el computador de

inmediato, desconectar en forma física el equipo de todas las redes y llamar al Centro de Atención al Usuario [insertar su número de teléfono o un enlace a su página intranet]. En caso de que el virus sospechoso pareciera estar ocasionando daños en la información o en el software, se deberá apagar el computador personal de inmediato.

Diversión con Virus—Los usuarios no deben escribir, compilar, copiar, propagar, ejecutar o intentar introducir en forma intencional algún código de programación diseñado para auto-duplicarse, dañar o entorpecer el desempeño de cualquier sistema de computación de la Empresa X.

RESPALDO

Copias en Archivo—Todo software de computadores personales distinto al software normativo de la Compañía X debe copiarse con anterioridad a su uso inicial y almacenarse en un sitio seguro. Estas copias maestras, posiblemente los mismos medios suministrados por el proveedor, no deben usarse para actividades empresariales ordinarias, sino más bien reservarse para realizar la recuperación en caso de producirse infecciones por virus, colapsos del disco duro y otros problemas. La documentación sobre las licencias del mencionado software se debe guardar para obtener apoyo técnico, recibir descuentos en actualizaciones y verificar la validez legal de las licencias.

Respaldo Periódico—Toda información importante, valiosa o confidencial que resida en los sistemas de computación de la Compañía X debe respaldarse periódicamente, por lo menos semanalmente. A menos que se cuente con sistemas automáticos de respaldo, todos los usuarios finales tienen la responsabilidad de hacer por lo menos una copia de respaldo actualizada de los archivos importantes, valiosos o confidenciales. Estas copias separadas de respaldo deberían hacerse cada vez que se guarda un número significativo de cambios. Los respaldos generados por el usuario deben almacenarse fuera de la oficina en un lugar físicamente seguro. Algunos archivos respaldados deben ser restaurados periódicamente para demostrar la eficacia de cada proceso de respaldo. Los gerentes de los distintos

departamentos deben verificar que se realizan respaldos adecuados en todos los computadores personales utilizados para las actividades empresariales de producción. El soporte técnico del Centro de Atención al Usuario está disponible para aquellos trabajadores que tengan dificultad para especificar, configurar o de algún otro modo establecer sistemas de respaldo.

Informe de Compras de Software—Todas las compras efectuadas por los departamentos usuarios de software para computadores personales que no hayan sido canalizadas a través del departamento de Compras, deben informarse con prontitud al Centro de Atención al Usuario del departamento de Sistemas Informáticos.

Protección de Derechos Reservados—Queda prohibido realizar copias de software que tengan licencias y derechos reservados, aun con propósitos de "evaluación". La Empresa X permite la reproducción de materiales con derechos reservados solamente hasta lo que legalmente se considera uso razonable o con permiso del autor o propietario. Si los trabajadores tienen alguna pregunta acerca de las leyes sobre derechos reservados, deben ponerse en contacto con el asesor legal corporativo. Salvo que reciban información que indique lo contrario, los trabajadores deben asumir que el software y otros materiales tienen derechos reservados.

DESTRUCCIÓN

Eliminación de Información Usada—Los trabajadores deben eliminar información de sus computadores personales si consideran que ya no se necesita o no tiene una utilidad potencial. Antes de eliminar cualquier

información, los trabajadores deben consultar el Cronograma de Retención de Documentos preparado por el asesor legal corporativo [aquí se puede insertar un enlace intranet]. El uso de una sola opción de borrado no

es suficiente para eliminar la información confidencial, puesto que ésta puede ser recuperable y debe eliminarse con un programa de reescritura autorizado por el departamento de Seguridad Informática [aquí se puede insertar un enlace a la lista de productos autorizados].

Destrucción de Información—Antes de desecharse, los discos flexibles defectuosos o dañados que contengan información confidencial deben destruirse usando tijeras u otros métodos autorizados por el

departamento de Seguridad Informática. Otros medios de almacenamiento que contengan información confidencial se deben desechar en los recipientes de destrucción cerrados bajo llave que se encuentran en las oficinas de la Compañía X. Todas las copias en papel que contengan información confidencial se deben desechar, bien sea en estos recipientes o en las máquinas trituradoras de papel autorizadas para tal fin.

DOCUMENTACIÓN

Documentación para los Sistemas de Producción—Todo usuario que desarrolle o implemente software o hardware para uso de la Compañía X en sus actividades empresariales de producción, debe documentar el sistema previo a su utilización. La documentación debe escribirse de forma tal que pueda ser utilizada por personas que no estén familiarizadas con el sistema. La documentación debe prepararse aun en aquellos casos en los que se emplee un software común, como por ejemplo un programa de hoja de cálculo.

Convenciones de Desarrollo de Sistemas de Producción—Todos los trabajadores que desarrollen o actualicen aplicaciones de producción de la Empresa X que se ejecutan en un computador personal, deben cumplir con los requerimientos abreviados de desarrollo de sistemas del departamento de Sistemas de Información. Estos requerimientos abreviados han sido preparados específicamente para los computadores personales y requieren mucho menos esfuerzo que los sistemas multiusuario e incluyen una evaluación de

riesgo, una revisión rápida para asegurar que dicho sistema de producción cumple con las normas técnicas existentes y el uso de nombres de archivo normalizados.

Planes de Contingencia—Cuando se utiliza un computador personal como parte fundamental de cualquier aplicación empresarial de producción, debe existir un plan de contingencia documentado y comprobado. Los planes de contingencia deben prepararse de acuerdo con los lineamientos establecidos por el departamento de Seguridad Informática [aquí se puede insertar un enlace intranet].

Etiquetado Uniforme de la Clasificación—Desde el momento en que se genera la información confidencial hasta el momento en que se destruye o se autoriza el libre acceso a ella, debe etiquetarse con una identificación correspondiente a su contenido, la cual debe aparecer en las versiones impresas y en las etiquetas de los medios de almacenamiento que contengan dicha información. Para obtener información adicional acerca de la clasificación de información y su identificación, ver la Política de Clasificación de la Información [aquí se puede insertar un enlace intranet].

TRABAJO EN REDES

Módem—Queda prohibido el uso de cualquier módem dentro o agregado a los computadores personales de la Empresa X, a excepción de los computadores portátiles y los de teletrabajo. El software de comunicaciones debe emplear siempre una contraseña de por lo menos diez caracteres creada de acuerdo con las reglas descritas en otra sección de este documento. Cuando los usuarios se encuentren en las oficinas de la Empresa X y tengan la necesidad de realizar conexiones salientes con computadores remotos, deben enrutarlas a través de los grupos de modem o del cortafuego de Internet.

Internet—Quedan prohibidas las conexiones entrantes de Internet a los computadores personales de la Compañía X, salvo que dichas conexiones empleen un paquete de software de red privada virtual (VPN, por sus siglas en inglés) autorizado por el departamento de Seguridad Informática. Estos sistemas VPN deben contar con las siguientes dos características: opciones de autenticación de usuario con por lo menos contraseñas fijas, y opciones de prevención de interceptación de datos como, por ejemplo, el cifrado.

Descarga de Información Confidencial—La información confidencial de la Empresa X se puede descargar desde un sistema multiusuario a un computador personal únicamente si se establece claramente que es necesaria para el negocio, si los controles de protección adecuados están instalados actualmente en el computador personal y si se obtiene el permiso del Propietario de la información. Esta política no abarca el correo electrónico ni los memos pero sí las bases de datos, los archivos maestros y otros datos almacenados en los mainframes, los minicomputadores, los servidores y otros equipos multiusuario, independientemente de los medios en los que se encuentre almacenada la información, la tecnología de sistemas usada para procesarla, la gente que la maneja o los procesos mediante los cuales se maneja.

Instalación de Líneas de Comunicación—Los trabajadores y los proveedores no deben hacer arreglos para la instalación de líneas de datos o de voz con ninguna empresa de telecomunicaciones, si no han obtenido la autorización del director del departamento de Sistemas Informáticos.

Establecimiento de Redes—Los trabajadores no deben establecer sistemas de foros o boletines electrónicos, redes de área local, sistemas de comercio por Internet y otros sistemas multiusuario para comunicar información, sin la autorización específica del departamento de Seguridad Informática.

Sincronización Automática de Dispositivos—No deben activarse los sistemas que intercambian datos en forma automática entre dispositivos, como por ejemplo un asistente digital personal y un computador personal, a menos que hayan sido evaluados y autorizados por el departamento de Seguridad Informática.

SEGURIDAD FÍSICA

Robo de Equipos—Todos los computadores personales, a excepción de los portátiles, deben asegurarse a los escritorios con dispositivos autorizados, tales como sujetadores o placas que inmovilicen el equipo. Todos los equipos deben marcarse con datos de identificación invisibles que indiquen claramente que son propiedad de la Empresa X. Adicionalmente, se deben llevar a cabo inventarios físicos periódicos para seguir el movimiento de los computadores personales y los periféricos correspondientes.

Donación o Venta de Equipos—Antes de entregar a un tercero los computadores personales o los medios de almacenamiento que hayan sido utilizados por la Empresa X, el departamento de Seguridad Informática debe realizar una inspección física para determinar que toda la información confidencial ha sido eliminada. Esta política no es aplicable si el tercero firmó un acuerdo de confidencialidad.

Préstamos de Computadores Personales a Otros—Los trabajadores nunca deben prestar a otra persona un computador personal de la Empresa X que contenga información confidencial, a menos que esa persona haya recibido una autorización previa por parte del Propietario de la información para acceder a ella.

Custodios de los Equipos—El usuario primario de un computador personal es considerado el custodio del equipo. Si el equipo ha sido dañado, perdido, robado o no está disponible por algún otro motivo para las actividades normales del negocio, el Custodio debe

informar con prontitud al gerente del departamento correspondiente. A excepción de los equipos portátiles, el computador personal no debe moverse o ubicarse en otro lugar sin el conocimiento y autorización del gerente del departamento.

Uso de Equipos Personales—Los trabajadores no deben traer a las instalaciones de la Empresa X sus computadores, periféricos o software sin la autorización previa del jefe de su departamento, ni tampoco usar sus computadores personales para el negocio de producción de la Empresa X, a menos que estos sistemas hayan sido evaluados y autorizados por el departamento de Seguridad Informática. Para los efectos de esta política, el redactar memos o informes no se considera parte del negocio de producción de la Empresa X.

Autorización para Mover Propiedad—Los computadores personales y portátiles, las máquinas de escribir y otros equipos de sistemas informáticos similares, así como los equipos que pertenecen a los trabajadores y que hayan sido traídos a las oficinas de la Empresa X, no deben salir de las mismas a menos que estén acompañados de una autorización firmada por el gerente del departamento. El personal de seguridad ubicado en la entrada de todos los edificios de la Empresa X debe revisar el contenido de los maletines, las maletas, los bolsos y otro tipo de equipaje para asegurarse de que todos los equipos que salen de las oficinas de la Empresa X tienen un pase autorizado. Se debe instalar

dispositivos sensores remotos en lugares seleccionados para activar una alarma si se extrae algún dispositivo relacionado con los computadores de la Empresa X.

Colocación de las Pantallas—Las pantallas de todos los computadores que manejan datos confidenciales o valiosos deben colocarse de tal manera que la información no pueda ser vista con facilidad a través de una ventana ni por personas que caminen por el pasillo o que se encuentran esperando en la recepción y áreas similares. Igual cuidado debe tenerse al colocar los teclados para evitar que las personas no autorizadas puedan ver con facilidad a los trabajadores mientras éstos ingresan sus contraseñas, sus claves de cifrado y otros parámetros de seguridad.

Resguardo de Información Confidencial—Todo material impreso que contenga información confidencial debe guardarse en archivos, escritorios, cajas fuertes u otro tipo de mobiliario cuando los trabajadores autorizados no lo estén usando o cuando no quede claramente a la vista en el área correspondiente. En cualquiera de los casos mencionados con anterioridad,

todos los medios de almacenamiento que contengan información confidencial deben resguardarse en recintos similares.

Consideraciones Ambientales—Todos los computadores personales de las oficinas de la Empresa X deben usar reguladores de voltaje y aquéllos que ejecutan aplicaciones de producción deben, además, poseer sistemas de energía ininterrumpida autorizados por el departamento de Seguridad Informática.

Descargas Estáticas y Campos Electromagnéticos—Cuando las condiciones del tiempo y las de la edificación representen un riesgo significativo de descarga de electricidad estática, los computadores personales deben estar provistos de un equipo anti-estática autorizado por el departamento de Sistemas de Información. Los medios de almacenamiento magnéticos tales como los discos flexibles y las cintas magnéticas deben guardarse a una distancia mínima de varios centímetros de los campos eléctricos, tales como los generados por imanes y teléfonos.

Cigarrillos, Comidas y Bebidas—Los trabajadores deben abstenerse de fumar, comer o beber cuando estén usando los computadores personales.

GESTIÓN

Derechos sobre los Programas Desarrollados—Salvo que exista una excepción específica por escrito, todos los programas de computación y la documentación generada o suministrada por los trabajadores para el beneficio de la Empresa X son propiedad de ésta, al igual que todos los otros materiales, incluyendo patentes, derechos reservados y marcas registradas desarrollados por los trabajadores de la Empresa X en sus computadores personales.

Exploración—Los trabajadores no deben explorar los sistemas de computación o las redes de la Empresa X. Las gestiones que el trabajador realice para encontrar en forma legítima la información necesaria para llevar a cabo su trabajo y el uso de la intranet de la Empresa X no se considera exploración.

Herramientas que Comprometen la Seguridad de los Sistemas—A menos que el departamento de Seguridad Informática lo autorice específicamente, los trabajadores de la Empresa X no deben adquirir, poseer, intercambiar o usar herramientas de hardware o software que pudiesen emplearse para evaluar o comprometer la seguridad de los sistemas informáticos; entre ellas, aquéllas que pudiesen vulnerar la protección

contra el copiado del software, descifrar contraseñas secretas, identificar vulnerabilidades en la seguridad o descifrar archivos cifrados.

Informe de Problemas—Los usuarios deben informar con prontitud todos los alertas de seguridad, las advertencias y las sospechas de vulnerabilidades al Centro de Atención al Usuario de Sistemas Informáticos, y no deben usar los sistemas de la Empresa X para enviar esta información a otros usuarios, sin importar si son internos o externos.

Información Adicional—Cada departamento debe designar un oficial de enlace de seguridad informática quien deberá ser la persona a la cual el lector se dirigirá en primer término, de requerir información adicional. Si este enlace no puede responder a la pregunta o brindar una resolución satisfactoria al problema, el próximo paso es llamar al departamento de Seguridad Informática corporativa al XXX-XXX-XXXX.

Aprobado por : [insertar nombre de ejecutivo]

Fecha de Aprobación: DD/MM/AA

Fecha de Vigencia: DD/MM/AA

Número de Versión: XX



Capítulo 9 MODELO DE POLÍTICA DE CORREO ELECTRÓNICO

Propiedad de la Empresa—Como herramienta para aumentar la productividad, la Empresa X estimula el uso empresarial de los sistemas de comunicación electrónica, especialmente la Internet, el teléfono, el buscapersonas, el correo de voz, el correo electrónico y el fax. Salvo en el caso de que terceros hayan hecho valer sus derechos reservados, o algún otro derecho, en los mensajes manejados por estos sistemas, todos los mensajes generados o manejados por la Empresa X se consideran propiedad de ésta.

Uso Autorizado—En términos generales, los sistemas de comunicación electrónica de la Empresa X deben usarse únicamente para actividades empresariales. El uso personal adicional es permitido siempre y cuando sólo consuma una cantidad mínima de los recursos del sistema, no interfiera con la productividad del trabajador y no tenga prioridad sobre otras actividades del negocio. Los sistemas de comunicación electrónica no deben usarse para la organización de campañas de recaudación de fondos para obras benéficas, actividades para la defensa de intereses políticos o religiosos, actividades privadas de negocios o entretenimiento personal. Las fuentes de noticias, listas de direcciones de correo electrónico, actualizaciones automáticas de datos y otros mecanismos para la recepción de información a través de la Internet deben restringirse a materiales que estén relacionados directamente con el negocio de la Empresa X y las tareas de los destinatarios. Se recuerda a los trabajadores que el uso de los recursos corporativos del sistema de información nunca debe crear la impresión o la realidad de que se están empleando indebidamente.

Privilegios Predeterminados—Los sistemas de comunicación electrónica deben establecerse y mantenerse de tal forma que solamente se otorguen al trabajador los privilegios necesarios para llevar a cabo su trabajo. Por ejemplo, al momento de terminar la relación entre el trabajador y la Empresa X, también deben cesar todos los privilegios del trabajador en los sistemas de comunicación electrónica de la Empresa X. Salvo en casos de emergencia y en los avisos de mantenimiento regular del sistema, las facilidades de transmisión deben usarse solamente después de haber obtenido el permiso del gerente de un departamento.

Separación de Usuarios—Estas opciones deben implementarse en aquellos casos en los que los sistemas de comunicación electrónica permitan separar las

actividades de diferentes usuarios. Por ejemplo, los sistemas de correo electrónico deben utilizar los identificadores de usuario y las contraseñas correspondientes. A menos que se utilice un sistema computarizado de buzón de fax, los equipos de fax que, por lo general, no tienen buzones separados para destinatarios diferentes no requerirán de esta opción. Si la Empresa X ha establecido la separación de usuarios, los trabajadores no deben emplear el identificador de ningún otro usuario.

Responsabilidad del Usuario—Independientemente de las circunstancias, las contraseñas individuales nunca deben compartirse o revelarse a ninguna persona, excepto al usuario autorizado. El personal del departamento de Tecnología de Información no debe pedir a los usuarios que revelen sus contraseñas. Cuando éstos necesiten compartir datos que se encuentran en el computador, deben utilizar las opciones de reenvío de mensajes, los directorios públicos en servidores de red de área local, las bases de datos grupales y otros mecanismos autorizados para compartir la información. Para impedir que partes no autorizadas obtengan acceso a las comunicaciones electrónicas, las contraseñas elegidas por los usuarios deben ser difíciles de adivinar. Por ejemplo, los usuarios no deben incluir palabras que se encuentran en diccionarios, datos personales, nombres o algún otro término relacionado con las actividades del trabajo.

Identidad del Usuario—Queda prohibido falsear, confundir, ocultar o sustituir la identidad de otro usuario en un sistema de comunicaciones electrónicas. El nombre del usuario, la dirección de correo electrónico, la afiliación a una organización y otros datos relacionados incluidos en los mensajes o anuncios electrónicos deben señalar el verdadero origen de los mismos. A excepción de las líneas calientes cuyo propósito es el anonimato, los trabajadores no deben enviar comunicaciones electrónicas anónimas. Como mínimo, todos los trabajadores deben suministrar su nombre y número de teléfono en todas estas comunicaciones electrónicas. Además, se recomiendan las firmas en el correo electrónico indicando el cargo, la afiliación a la empresa, la dirección y otros detalles así como las certificaciones digitales para todos los mensajes de correo electrónico.

Uso Único de los Sistemas de Correo Electrónico de la Empresa X—Salvo que se obtenga un permiso del gerente de Seguridad Informática, los trabajadores no deben usar sus cuentas personales de correo electrónico para los mensajes empresariales de la Empresa X ni las opciones de correo electrónico que se encuentran en los exploradores de la web para las comunicaciones de la Empresa X. Solamente deben emplear el software de correo electrónico autorizado por la Empresa X.

Uso de Programas de Cifrado—Se recuerda a los trabajadores de la Empresa X que los sistemas de comunicación electrónica no están cifrados de manera predeterminada. Si los sistemas de comunicación electrónica deben enviar Información Confidencial o Secreta, se debe emplear un proceso de cifrado autorizado por el departamento de Seguridad Informática. Estos sistemas deben proteger la información en toda su extensión y no deben comprometer la decodificación del contenido del mensaje antes de que el mismo llegue a su destino final. Los computadores portátiles, los asistentes personales digitales (de bolsillo tipo Palm) y equipos similares que almacenan información confidencial de la Empresa X, deben emplear constantemente el cifrado de archivos para proteger esta información cuando se almacena en estos computadores y cuando se almacena en medios adjuntos de almacenamiento de datos. Los usuarios de estos tipos de computadores que reciben información confidencial enviada por correo electrónico deben eliminar esta información de sus sistemas si no tienen el software de cifrado que la pueda proteger adecuadamente. Los trabajadores no deben usar el cifrado para ningún sistema de comunicaciones electrónicas de producción a menos que se haya establecido una clave de respaldo o un sistema de garantía de claves con la colaboración de Seguridad Informática.

Etiquetado de los Mensajes de Correo Electrónico—Todos los mensajes de correo electrónico que contengan información confidencial deben incluir la clasificación adecuada en el encabezado. Esta etiqueta servirá como recordatorio a los destinatarios de que la información no debe difundirse o usarse para propósitos no establecidos sin la debida autorización.

Respeto a los Derechos de Propiedad Intelectual—Aun cuando la Internet es un ambiente informal de comunicaciones, también hay que cumplir las leyes de derechos reservados, patentes y marcas registradas. Los trabajadores que usen los sistemas de correo electrónico de la Empresa X solamente deben reenviar o reproducir material después de obtener el permiso de la fuente, citar material de otras fuentes sólo si éstas se logran identificar adecuadamente o revelar la

información interna de la Empresa X en la Internet únicamente cuando haya sido autorizada oficialmente su divulgación pública. Toda información adquirida de Internet se debe considerar no confiable hasta que haya sido confirmada por otra fuente.

Respeto del Derecho a la Privacidad—Salvo que el gerente de Seguridad Informática lo autorice específicamente de otra manera, los trabajadores no deben interceptar, revelar, ni contribuir en la interceptación o revelación de las comunicaciones electrónicas. La Empresa X se compromete a respetar los derechos de sus trabajadores incluyendo el respeto a su privacidad e igualmente se responsabiliza de la operación, el mantenimiento y la protección de sus redes de comunicaciones electrónicas. Para alcanzar estos objetivos, en ocasiones será necesario interceptar o revelar o contribuir en la interceptación o revelación de las comunicaciones electrónicas, para lo cual la Empresa X puede emplear sistemas de evaluación de contenido, sistemas de registro de mensajes y otras herramientas de gestión de sistemas electrónicos. Al hacer uso de los sistemas de la Empresa X, los usuarios dan su consentimiento para que toda la información que ellos almacenen en los sistemas se divulgue a las autoridades pertinentes, a discreción de la gerencia de la Empresa X.

No se Garantiza la Privacidad de los Mensajes—La Empresa X no puede garantizar que las comunicaciones electrónicas sean privadas. Los trabajadores deben saber que las comunicaciones electrónicas pueden, dependiendo de la tecnología, ser reenviadas, interceptadas, impresas y guardadas por otros y que personas distintas a los destinatarios pueden acceder a las comunicaciones electrónicas por efecto de esta política. Debido a que los mensajes se pueden almacenar en respaldos, las comunicaciones electrónicas pueden de hecho ser recuperadas, mientras que una carta tradicional en papel se hubiera podido descartar o destruir. Los trabajadores deben tener cuidado con los asuntos tratados en las comunicaciones electrónicas de la Empresa X y no deben enviar ningún mensaje cuyo contenido les pudiese causar incomodidad al verlo publicado en la primera página del periódico.

Contenido de los Mensajes—Los trabajadores no deben usar frases irreverentes, palabras obscenas o comentarios peyorativos en los mensajes de correo electrónico en referencia a los empleados, los clientes, los competidores u otras personas, ya que esos comentarios pueden crear problemas legales tales como la difamación y la calumnia en contra de empresas y personas. En las comunicaciones electrónicas de la Empresa X, los trabajadores deben ocuparse de los asuntos relacionados con el negocio. Como parte de las

prácticas normales de las actividades del negocio, todas esas comunicaciones deben adherirse a las normas convencionales de conducta, de ética y de cortesía.

Datos Estadísticos—De acuerdo con las prácticas comerciales generalmente aceptadas, la Empresa X recopila datos estadísticos sobre sus sistemas de comunicaciones electrónicas. Mediante el empleo de estos datos, el personal de soporte técnico evalúa el uso de las comunicaciones electrónicas para asegurar la continua disponibilidad, confiabilidad y seguridad de estos sistemas. La Empresa X emplea sistemas de computación que analizan estos datos estadísticos para detectar usos no autorizados, fraudes, ataques de negación de servicio y otros problemas.

Divulgación Incidental—El personal de soporte técnico no debe revisar el contenido de las comunicaciones de un trabajador en particular, bien por simple curiosidad o a solicitud de individuos que no hayan utilizado los canales adecuados. Para realizar esta evaluación, se requiere una autorización previa del gerente de Seguridad Informática.

Notas en el Correo Electrónico Saliente—Una nota al pie, preparada por el departamento Legal, debe anexarse en forma automática a todo el correo electrónico de salida que se genera desde los computadores de la Empresa X. Esta nota debe hacer referencia a la posibilidad de que el mensaje contenga información confidencial, que es para el uso exclusivo de los destinatarios mencionados, que ha sido archivado para fines de respaldo, que puede ser revisado por personas en la Empresa X distintas a las nombradas en el encabezado y que no constituye necesariamente una representación oficial de la Empresa X.

Manejo de los Archivos Anexos—Cuando los trabajadores envíen archivos adjuntos a un tercero, deben tratar de usar un formato de texto amplio o archivos de texto simple cada vez que sea posible. De igual manera, deben estimular a los terceros para que utilicen este mismo formato en los archivos que les envían cuando se considere práctico y razonable. Todos los demás archivos adjuntos deben ser examinados con un paquete de software antivirus autorizado antes de abrirlos o ejecutarlos. En algunos casos, los archivos adjuntos deben descifrarse o descomprimirse antes de realizarse la verificación de virus. Los trabajadores deben desconfiar de los archivos adjuntos recibidos de terceros, aun cuando los conozcan y confien en ellos.

Reenvío de Mensajes—Los usuarios de las comunicaciones electrónicas deben ser precavidos cuando reenvíen los mensajes. La información Confidencial o

Secreta de la Empresa X no debe enviarse a ningún tercero fuera de la Empresa X sin la autorización previa de un gerente departamental. Queda prohibido el reenvío general de mensajes a terceros fuera de la Empresa X a menos que se haya obtenido un permiso con anticipación del gerente de Seguridad Informática. Los mensajes enviados por terceros no deben reenviarse a otros terceros salvo que el remitente tenga un claro propósito y el envío es necesario para alcanzar los objetivos empresariales normales. En todos los demás casos, el reenvío de mensajes enviados por personas fuera de la Empresa a otros terceros sólo debe realizarse si el remitente está expresamente de acuerdo con dicho reenvío.

Manejo de Alertas de Seguridad—Los usuarios deben reportar con prontitud todos los alertas de seguridad, advertencias y vulnerabilidades al departamento de Seguridad Informática, el cual es la única unidad autorizada de la organización que puede definir el curso de acción conveniente para responder a estos avisos. Los usuarios no deben utilizar los sistemas de la Empresa X para reenviar estos avisos a otros usuarios, bien sea internos o externos a la Empresa X y deben reportar con prontitud a Seguridad Informática todos los aspectos que ellos consideren vulnerables en cuanto a seguridad o cualquier otro problema que identifiquen [aquí se puede insertar un enlace intranet a un formulario para el reporte de problemas].

Representaciones Públicas—No puede realizarse ninguna representación pública sobre la Empresa X en los medios de comunicación, en la página inicial de Internet, en los foros o boletines electrónicos, en los mensajes de correo electrónico, ni en los mensajes de correo de voz a menos que haya sido autorizada por los departamentos de Mercadeo y de Relaciones Públicas. Como parte de la política, la Empresa X no envía correo electrónico ni publicidad por fax no solicitados. Ninguna persona fuera de la Empresa X puede ser añadida a una lista de envío de correo electrónico si no ha manifestado su intención de ser incluida mediante un proceso de suscripción. Si los trabajadores de la Empresa X están abrumados debido a una cantidad excesiva de mensajes no deseados de una organización en particular o de una dirección de correo electrónico, no deben responder directamente al remitente. Los destinatarios deben reenviar ejemplos de los mensajes al administrador del sistema encargado del sistema de correo electrónico para buscar una solución. Los trabajadores no deben enviar un gran número de mensajes con el objeto de sobrecargar un servidor o el buzón de correo electrónico de un usuario como medida de retaliación por algún asunto que hayan notado.

Respaldo del Usuario—Si un mensaje de correo electrónico contiene información esencial para completar una transacción de negocios, información de referencia de importancia potencial o que sea valiosa como prueba para sustentar decisiones tomadas por la gerencia de la Empresa X, se debe guardar para referencias futuras. Los usuarios deben trasladar con regularidad la información de los archivos de mensajes de correo electrónico a documentos procesados en texto, bases de datos y otros archivos. Las bandejas de entrada del correo electrónico no deben usarse para el almacenamiento de información importante.

Almacenamiento de Archivos—Todos los mensajes oficiales de correo electrónico de la Empresa X, incluyendo aquéllos que contienen una aprobación formal, autorización, delegación o manejo de las responsabilidades o transacciones similares emanadas de la gerencia, deben copiarse al departamento de Registro de Archivos. Todos los contratos legales, estados financieros, anuncios públicos, anuncios de empleo, declaraciones de impuesto y otras comunicaciones deben enviarse a Registro de Archivos.

Eliminación de Mensajes Electrónicos—Los usuarios deben eliminar periódicamente de sus espacios de almacenamiento de mensajes electrónicos, los mensajes que ya no se necesiten para efectos empresariales. Luego de seis meses de estar almacenados en los servidores de la Empresa X, los mensajes de correo electrónico deben ser eliminados por el personal de administración del sistema.

Materiales Ofensivos—Los sistemas de comunicaciones y de computación de la Empresa X no están destinados ni deben usarse para el ejercicio del derecho a la libre expresión del trabajador. Estos sistemas no deben usarse como un foro abierto para discutir cambios organizacionales de la Empresa X o asuntos de política de los negocios. Queda estrictamente prohibido el acoso sexual, étnico y racial incluyendo llamadas telefónicas, correo electrónico y correo interno no deseados. Los trabajadores que reciban material ofensivo no solicitado proveniente de fuentes externas no deben reenviarlo o redistribuirlo, bien sea a personas dentro de la empresa o a terceros a menos que este reenvío o redistribución se haga al departamento de Recursos Humanos de la Empresa X con el objeto de colaborar en la investigación de quejas.

Respuesta Directa al Remitente—Los trabajadores deben responder directamente al autor de los mensajes de correo electrónico, llamadas telefónicas y otras comunicaciones que contengan material ofensivo. Si éste no deja de enviar los mensajes ofensivos con prontitud, los trabajadores deben reportar las comunicaciones a su gerente y al departamento de Recursos Humanos. La Empresa se reserva el derecho de remover de sus sistemas de información cualquier material que considere ofensivo o potencialmente ilegal.

Uso por Cuenta y Riesgo—Los trabajadores acceden a la Internet con las facilidades de la Empresa X bajo su propia responsabilidad. La Empresa X no es responsable del material visto, descargado o recibido por los usuarios a través de la Internet. Los sistemas de correo electrónico pueden presentar mensajes no solicitados con contenido ofensivo.

Establecimiento de Sistemas de Negocios Electrónicos—Aun cuando la Empresa X implemente un Intercambio de Datos Electrónicos (EDI, Electronic Data Interchange, por sus siglas en inglés), comercio en Internet y otros sistemas de negocios electrónicos con terceros, todos los contratos deben formalizarse mediante documentos en papel antes de comprar o vender a través de los sistemas electrónicos. El EDI, el correo electrónico y otros mensajes de negocios similares vinculantes deben recibirse contra pedidos generales, como por ejemplo, un pedido de compra general. Todos los sistemas de comercio electrónico deben estar autorizados por el ejecutivo oficial de información, el gerente de Seguridad Informática y el ejecutivo asesor legal antes de su uso.

Confirmación en Papel de Contratos—Todos los contratos hechos a través de una oferta electrónica y de mensajes de aceptación deben formalizarse y confirmarse mediante documentos escritos en papel dentro de las dos semanas siguientes a la fecha de aceptación. Los trabajadores no deben emplear versiones escaneadas de firmas manuscritas para dar la impresión de que un mensaje de correo electrónico y otras comunicaciones electrónicas fueron firmados por el remitente.

Aprobado por: [insertar nombre de ejecutivo]

Fecha de Aprobación: DD/MM/AA

Fecha de Vigencia: DD/MM/AA

Número de Versión: XX

Número de Referencia de Documento : XXXX-XXXX



Capítulo 10 MODELO DE POLÍTICA DE SEGURIDAD EN REDES DE COMPUTACIÓN

PROPÓSITO

El propósito de esta política es establecer la dirección gerencial, los requisitos procedimentales y la orientación técnica para garantizar la protección adecuada de la

información manejada en las redes de computación de la Empresa X.

ALCANCE

Esta política se aplica a todos los empleados, contratistas, consultores, personal temporal, voluntarios y otros trabajadores de la Empresa X, incluyendo aquellos trabajadores afiliados a terceros que accedan a las redes de computación de la Empresa X. En toda la extensión

de esta política, la palabra "trabajador" se empleará en forma colectiva para referirse a todos estos individuos. Esta política también se aplica a todos los sistemas de computación y de comunicaciones de datos que sean propiedad o estén administrados por la Empresa X.

POLÍTICA GENERAL

Toda la información que viaje a través de las redes de computación de la Empresa X que no haya sido identificada específicamente como propiedad de otras partes, se tratará como si fuera un activo corporativo de la Empresa X. Es la política de la Empresa X prohibir el acceso no autorizado, la divulgación, la duplicación, la modificación, la desviación, la destrucción, la pérdida,

el uso indebido o el robo de esta información. Adicionalmente, ésta es la política de la Empresa X para proteger la información que pertenece a terceros y que ha sido confiada a la Empresa X, de manera consistente con su confidencialidad y en consonancia con todos los acuerdos que se apliquen.

RESPONSABILIDADES

Un comité de gerencia de seguridad informática integrado por gerentes medios o sus delegados de cada división y subsidiaria de importancia, el director de Tecnología de Información, el director de Seguridad y el ejecutivo asesor legal de la Empresa X responsable de la propiedad intelectual, revisará periódicamente, en reuniones trimestrales y ad hoc, el estado de la seguridad de las redes y los computadores de la Empresa X, estudiará y evaluará el trabajo de recuperación relacionado con incidentes de seguridad de las redes y los computadores, autorizará y posteriormente emitirá juicio sobre los resultados de los proyectos importantes relacionados con la seguridad de las redes y los computadores, aprobará políticas, normas, lineamientos y procedimientos nuevos o modificados en materia de seguridad informática y realizará otras actividades gerenciales de alto nivel en esta materia.

El gerente de Seguridad Informática tiene la responsabilidad de establecer, mantener, implementar, administrar e interpretar políticas, normas, lineamientos y procedimientos relativos a la seguridad de los sistemas informáticos en toda la extensión de la organización, así como todas las actividades relacionadas con esta política. Mientras que la responsabilidad por la seguridad de los sistemas informáticos es un deber diario del trabajador, la orientación específica, la dirección y la autoridad por la seguridad de los sistemas informáticos para toda la Empresa X y sus subsidiarias está centralizada en el departamento de Seguridad Informática. Este departamento llevará a cabo evaluaciones de riesgo y preparará planes de acción de seguridad de los sistemas informáticos, evaluará productos de seguridad informática y realizará otras actividades necesarias para garantizar un ambiente seguro en los sistemas informáticos.

El gerente de Seguridad Física tiene la responsabilidad de conducir investigaciones referidas a los incidentes, los problemas y otros hechos que comprometan la seguridad de las redes y computadores. Todos los sucesos que comprometan o puedan comprometer la seguridad deben ser reportados de inmediato al gerente de Seguridad Física.

Los administradores del sistema tienen la responsabilidad de actuar como coordinadores locales de la seguridad de los sistemas informáticos. Estos individuos son responsables de establecer privilegios de usuario adecuados, de evaluar los registros de control de acceso y de llevar a cabo acciones de seguridad similares para los sistemas que ellos administran. Asimismo, son responsables de reportar todas las actividades sospechosas relacionadas con la seguridad de las redes y los computadores al gerente de Seguridad Física. Los administradores del sistema también implementan los requerimientos de ésta y otras políticas, normas, lineamientos y procedimientos de seguridad de los sistemas informáticos. Si la seguridad informática no es

manejada por otro grupo o departamento, cada departamento de la Empresa X debe designar a una persona para actuar como administrador del sistema.

Los gerentes de los departamentos tienen la responsabilidad de asegurar que las medidas de seguridad del sistema de comunicación y de los computadores se cumplan en sus áreas. Aparte de destinar recursos suficientes y tiempo del personal para cumplir con los requerimientos de estas políticas, los gerentes de los departamentos tienen la responsabilidad de asegurarse de que todos los usuarios tengan conocimiento de las políticas de la Empresa X relacionadas con la seguridad de los sistemas de comunicación y de los computadores.

Los usuarios tienen la responsabilidad de acatar ésta y otras políticas de la Empresa X que definen las medidas de seguridad de las redes y los computadores y de reportar todas las vulnerabilidades y las violaciones a la seguridad informática que ellos identifiquen, al gerente de Seguridad Física.

CONTROL DE ACCESO AL SISTEMA

Contraseñas de los Usuarios Finales

Los usuarios deben seleccionar contraseñas fijas que sean difíciles de adivinar, lo cual significa que las mismas no deben estar relacionadas con la vida personal o el trabajo del usuario, como por ejemplo, el número de placa de un automóvil, el nombre del cónyuge o fragmentos de una dirección, ni palabras incluidas en diccionarios o alguna parte gramatical tales como nombres propios, lugares, términos técnicos y jerga. Los usuarios deben abstenerse de elegir contraseñas que se pueden adivinar con facilidad en los lugares en donde este tipo de software de sistemas está disponible.

Los usuarios pueden seleccionar contraseñas fáciles de recordar, pero que sean difíciles de adivinar por terceros no autorizados, si:

- Enlazan varias palabras en una sola frase conocida sólo por ellos.
- Mueven una palabra una fila hacia arriba, hacia abajo, hacia la izquierda o hacia la derecha en el teclado.
- Mueven caracteres en una palabra varias letras en forma ascendente o descendente del alfabeto.

- Transforman una palabra normal siguiendo un método específico, como por ejemplo cambiando cada letra de por medio por un número que indique su posición en la palabra.
- Combinan signos de puntuación o números con una palabra normal.
- Crean siglas de palabras tomadas de una canción, un poema u otra secuencia conocida de palabras.
- Deletean mal una palabra deliberadamente.
- Combinan un número de datos personales como fechas de cumpleaños y colores favoritos.

Los usuarios no deben construir contraseñas que sean idénticas o similares a las empleadas con anterioridad. Los usuarios deben abstenerse de volver a usar contraseñas anteriores en los lugares en donde las facilidades de software de sistemas están disponibles.

Los usuarios no deben construir contraseñas usando una secuencia básica de caracteres que se modifica parcialmente basándose en la fecha o en algún otro factor predecible. Por ejemplo, los usuarios no deben emplear contraseñas tales como "X34ENE" en enero y "X34FEB" en febrero.

Las contraseñas no deben guardarse en forma legible en archivos por lotes, en resumen de comandos de inicio de sesión automático, en macros de software, en teclas de función, en software de comunicaciones de datos, en exploradores de la web, en unidades de disco duro o en otras ubicaciones donde personas no autorizadas puedan descubrirlas.

Las contraseñas no deben anotarse y dejarse en lugares donde personas no autorizadas puedan descubrirlas. Aparte de la asignación de la contraseña inicial y de las situaciones de reinicialización de la contraseña, si existiese alguna razón para creer que una contraseña ha sido revelada a alguna persona distinta al usuario autorizado, se debe cambiar inmediatamente.

Las contraseñas no deben compartirse o revelarse a ninguna otra persona aparte del usuario autorizado, así que, si los usuarios necesitan compartir datos que se encuentran en el computador, entonces deben usar el correo electrónico, los directorios públicos en los servidores de red de área local y otros mecanismos. Esta política no impide el uso de contraseñas predeterminadas, generalmente usados para la asignación de identificación de usuario nuevo o situaciones de reinicialización de la contraseña, las cuales se cambian de inmediato cuando el usuario vuelve a conectarse al sistema mencionado. Se deben cambiar todas las contraseñas cuando se sospeche que han sido reveladas o se tiene el conocimiento de que han sido reveladas a alguna persona distinta al usuario autorizado.

Instalación y Configuración del Sistema de Contraseñas

Todos los computadores que estén conectados en forma permanente o intermitente a las redes de la Empresa X deben tener controles de acceso de contraseñas. Si los computadores contienen información Confidencial o Secreta, se debe usar un sistema de autenticación extendida de usuario autorizado por el departamento de Seguridad Informática. En última instancia, los sistemas multiusuario deben emplear identificadores de usuario y contraseñas únicas para cada usuario y mecanismos de restricción de privilegios de usuario con privilegios basados en la necesidad del individuo de saber. Los sistemas de un solo usuario conectados a la red deben emplear controles de hardware o software autorizados por Seguridad Informática que impidan el acceso no autorizado incluyendo un protector de pantalla, el cual se activa después de cierto periodo de inactividad del teclado.

A menos que un sistema extendido de autenticación de usuario esté en uso, el control del acceso al sistema de comunicación y al computador debe lograrse mediante la utilización de contraseñas fijas que sean únicas para cada usuario en particular. Queda prohibido el control del acceso a archivos, aplicaciones, bases de datos, computadores, redes y otros recursos del sistema a través de contraseñas compartidas o contraseñas grupales.

Cuando el software del sistema lo permita, la presentación y la impresión de contraseñas fijas deben ocultarse de manera que las partes no autorizadas no puedan observarlas o recuperarlas posteriormente.

Cuando el software del sistema lo permita, las contraseñas fijas iniciales asignadas a un usuario nuevo por un administrador de seguridad deben tener validez únicamente para la primera sesión en línea del usuario.

En ese momento, se requerirá que el usuario elija otra contraseña. Este mismo proceso aplica a la reinicialización de contraseñas en la eventualidad de que un usuario olvide su contraseña.

Todas las contraseñas fijas predeterminadas suministradas por el proveedor deben modificarse antes de que cualquier sistema de comunicaciones o computador se empleen para el negocio de producción de la Empresa X. Esta política se aplica a contraseñas asociadas con identificadores de usuarios finales y contraseñas asociadas con identificadores de usuarios privilegiados.

Cuando el software del sistema lo permita, se debe limitar estrictamente el número de intentos consecutivos para ingresar una contraseña incorrecta. Luego de tres intentos fallidos para ingresar una contraseña, el identificador del usuario en cuestión debe suspenderse hasta que la reinicialice un administrador del sistema o inhabilitarse temporalmente por un lapso no menor de tres minutos. Si están en uso conexiones telefónicas, se debe desconectar la sesión. Si se emplean DSL, ISDN (red digital de servicios integrados), modem de cable u otras conexiones constantes, se debe iniciar un periodo de desconexión.

Cada vez que se haya comprometido la seguridad del sistema o cuando existan razones para creer que ha sido comprometida, el administrador del sistema afectado debe cambiar de inmediato todas las contraseñas de los usuarios privilegiados y solicitar que la contraseña de cada usuario final del sistema afectado se modifique para la próxima conexión de entrada. Si el software del sistema no brinda esta última capacidad, se debe enviar un mensaje de transmisión a todos los usuarios solicitándoles que cambien sus contraseñas de inmediato.

Cada vez que se haya comprometido la seguridad del sistema o cuando existan razones para creer que ha sido comprometida, una versión confiable del sistema operativo y todo el software relacionado con seguridad debe cargarse nuevamente desde medios de almacenamiento confiables tales como CD-ROM, cintas magnéticas o discos flexibles con código fuente original

Proceso de Inicio y Cierre de Sesión

Todos los usuarios deben identificarse positivamente antes de poder usar algún computador multiusuario y otros recursos del sistema de comunicaciones de la Empresa X. La identificación positiva para las redes internas de la Empresa X incluye un identificador de usuario y una contraseña fija, siendo ambos únicos para cada usuario individual o, en su defecto, un sistema extendido de autenticación de usuario.

La identificación positiva para todas las líneas discadas y de Internet incluye el uso de tarjetas portátiles, desafíos criptográficos, protocolos de respuestas cifradas u otras técnicas extendidas para la autenticación del usuario. La combinación de un identificador de usuario y una contraseña fija no brinda suficiente seguridad para las conexiones discadas o de Internet a los sistemas y las redes de la Empresa X. Queda prohibido el uso de modems agregados a las estaciones de trabajo conectadas a la red ubicadas en las oficinas de la Empresa X, a menos que tengan un sistema extendido de autenticación de usuario autorizado por el departamento de Seguridad Informática. Los modems conectados a computadores independientes tales como computadores portátiles y de uso doméstico son permitidos siempre y cuando se instale un cortafuego autorizado de computadores personales y el software de comunicaciones correspondiente no esté habilitado para recibir llamadas entrantes.

Cuando el software del sistema lo permita, cada mensaje de bienvenida mostrado en los computadores multiusuario debe incluir un aviso especial, el cual debe señalar que el sistema es para el uso exclusivo de usuarios autorizados y que de continuar usando el sistema, el usuario se presenta como un usuario autorizado, tiene conocimiento de que todo el uso del sistema se registra y entiende que las violaciones de las políticas de seguridad informática de la Empresa X y

y posteriormente se debe reinicializar el sistema afectado. El administrador del sistema debe revisar inmediatamente todos los cambios en los privilegios de los usuarios que tuvieron validez desde el momento de la sospecha de que el sistema estaba comprometido para verificar si hubo modificaciones no autorizadas.

otros requerimientos pueden ocasionar acciones disciplinarias, incluyendo el cese de la relación laboral y acciones legales.

El proceso de conexión para los sistemas de computación conectados a la red de la Empresa X debe simplemente pedirle al usuario que se conecte, suministrando mensajes según sea necesario. No debe suministrarse información específica que el computador contenga sobre la organización, el sistema operativo, la configuración de la red y otros asuntos internos, hasta que el usuario haya proporcionado con éxito una identificación de usuario y una contraseña válidas.

Si no ha habido actividad en un terminal, una estación de trabajo o un computador personal por cierto periodo de tiempo (el periodo de tiempo recomendado es de 15 minutos), el sistema debe obscurecer la pantalla en forma automática y suspender la sesión cuyo restablecimiento debe producirse solamente después de que el usuario haya suministrado una contraseña válida. De acuerdo con esta política, se podrá hacer excepciones en aquellos casos en donde el área inmediata que rodea a un sistema está físicamente asegurada con puertas cerradas, con lectores de distintivos o tecnologías similares.

Con la excepción de los foros y boletines electrónicos u otros sistemas en donde los usuarios regulares son anónimos, queda prohibido que los usuarios entren al sistema o a la red de la Empresa X en forma anónima, como por ejemplo, usando un identificador de usuario invitado. Si los usuarios emplean las facilidades de los sistemas para cambiar el identificador de usuario activo y así obtener ciertos privilegios, deben acceder inicialmente empleando un identificador de usuario que indique claramente su identidad.

Privilegios en el Sistema

Limitaciones de Acceso al Sistema

Los privilegios del sistema de comunicaciones y

computación de todos los usuarios, sistemas y programas que operan independientemente, tales como los agentes, deben restringirse a la necesidad de

conocer, lo cual significa que los privilegios no deben ser extendidos a menos que exista una necesidad legítima del negocio.

Los permisos predeterminados para ingresar a un archivo no deben permitir que ningún usuario del sistema lea, escriba, ejecute o elimine un archivo. Los permisos se otorgan a un grupo limitado de personas que tengan una verdadera necesidad de acceso. Queda prohibido que los usuarios reinicialicen los permisos archivo por archivo aunque puedan hacerlo.

Los usuarios con computadores personales tienen la responsabilidad de administrar un programa de protector de pantalla que proteja el acceso a la unidad de disco duro de su equipo y de fijar contraseñas para todas las aplicaciones y software de sistemas que brinden esa capacidad.

Los computadores y los sistemas de comunicación de la Empresa X deben restringir el acceso a los computadores que puedan alcanzar los usuarios a través de las redes de la Empresa X. Estas restricciones pueden implementarse a través de enrutadores, puertas de enlace, cortafuegos y otros componentes de la red y deben usarse, por ejemplo, para controlar la habilidad del usuario de iniciar sesión en un computador específico y, después, moverse desde ese computador a otro.

Proceso para Otorgar Privilegios en el Sistema

Las solicitudes para nuevos identificadores de usuario y modificaciones en los privilegios deben estar por escrito y autorizadas por el gerente del usuario antes de ser procesadas por el administrador del sistema. Los documentos de estas solicitudes deben conservarse por un periodo mínimo de un año.

Los individuos no empleados por la Empresa X no deben recibir un identificador de usuario ni privilegios para usar los computadores o redes de la Empresa X a menos que obtengan la autorización escrita de un jefe de departamento.

Los privilegios otorgados a usuarios no empleados de la Empresa X deben tener validez por períodos de 90 días o menos y, según sea necesario, deben pedir una nueva autorización de sus privilegios al jefe del departamento patrocinante cada 90 días.

Los privilegios especiales, como por ejemplo el de escribir en archivos de otros usuarios, se deben restringir a aquellas personas responsables de la administración o de la seguridad de los sistemas, pudiendo hacer excepciones cuando el jefe del departamento autorice por escrito. Los cambios en la

configuración, en el sistema operativo y en actividades relacionadas que requieran de privilegios en el sistema deben ser realizados por los administradores del sistema, no por los usuarios finales.

Los proveedores no deben recibir privilegios de discado o de Internet a los computadores y las redes de la Empresa X salvo que el administrador del sistema determine que tienen una necesidad justificada relacionada con los negocios. Estos privilegios deben habilitarse únicamente por el lapso de tiempo que se requiera para completar las tareas autorizadas, tal como el mantenimiento remoto. De necesitarse una conexión permanente o de largo plazo, ésta debe establecerse a través de métodos extendidos de autenticación de usuario.

Todos los usuarios que deseen usar las redes internas o los sistemas multiusuario de la Empresa X conectados a las redes internas de la Empresa X deben firmar una declaración de conformidad antes de recibir un identificador de usuario. Si un usuario en particular ya tiene un identificador de usuario, se debe obtener su firma antes de recibir la renovación, lo cual se debe realizar periódicamente.

Proceso para Revocar el Acceso al Sistema

Los privilegios asociados a todos los identificadores de usuario se deben revocar después de un periodo de inactividad que no exceda los 30 días.

Cuando un computador o un subsistema de control de acceso al sistema de comunicación no están funcionando adecuadamente, debe de manera predeterminada denegar los privilegios a los usuarios. Si los subsistemas de control de acceso no funcionan, no deben estar disponibles hasta que el problema se haya rectificado.

Los usuarios no deben hacer pruebas o poner en riesgo las medidas de seguridad del sistema de comunicación o del computador a menos que hayan recibido una autorización con anticipación y por escrito del gerente de Seguridad Informática. Los incidentes que incluyen el ingreso no autorizado al sistema, los intentos de adivinar la contraseña, el descifrado de archivos, las copias piratas de software o actos similares no autorizados que comprometan las medidas de seguridad pueden ser ilegítimas y se considerarán violaciones graves de la política de la Empresa X. Las solicitudes de clientes para comprometer los mecanismos de seguridad de la Empresa X no deben ser satisfechas, a menos que el gerente de Seguridad Informática lo autorice por anticipado o la Empresa X se vea obligada a cumplir por efecto de ley. Quedan terminantemente prohibidos los

atajos que vulneren las medidas de seguridad de los sistemas, así como las travesuras y bromas de mal gusto que pongan en riesgo la seguridad de los sistemas.

La gerencia debe reconsiderar cada seis meses los privilegios otorgados a los usuarios y los administradores del sistema deben revocar con prontitud todos los privilegios que los usuarios ya no necesiten.

La gerencia debe informar con prontitud todos los cambios significativos en los deberes del trabajador o en su situación laboral a los administradores del sistema responsables de los identificadores de usuario. Asimismo, al momento del cese de la relación laboral, el departamento de Recursos Humanos debe emitir una notificación a todos los administradores del sistema que pudiesen ser responsables de un sistema en el cual el trabajador referido podría tener un identificador de usuario

Establecimiento de Vías de Acceso

Las modificaciones a las redes internas de la Empresa X incluyen instalar un software nuevo, cambiar las direcciones de la red, reconfigurar enruteadores y agregar líneas de discado. Exceptuando las situaciones de emergencia, todos estos cambios deben documentarse en una solicitud de orden de trabajo y estar previamente autorizados por Tecnología Informática. Los cambios de emergencia a las redes deben ser realizados por personas autorizadas por este departamento. Este proceso evita problemas inesperados que abarcan desde la negación del servicio hasta la divulgación de la información. El proceso se aplica no sólo a los trabajadores sino también al personal del proveedor.

Los trabajadores no deben instalar sistemas de foros y boletines electrónicos, redes de área local, servidores de protocolo de transferencia de archivos (FTP), servidores web, conexiones modem a redes de área local existentes o algún otro sistema multiusuario para comunicar información ni establecer nuevos tipos de conexión en tiempo real entre dos o más sistemas internos de computación sin la autorización del gerente de Seguridad Informática.

Queda prohibida la participación en redes externas como proveedor de servicios a terceros hasta que el asesor legal de la Empresa X haya identificado los riesgos legales y el director de Tecnología Informática haya aceptado expresamente todos los riesgos relacionados con la propuesta.

Todos los computadores que se conectan a una red interna o externa deben emplear controles de acceso basados en contraseña o un sistema extendido de autenticación de usuario. Los computadores multiusuario deben emplear software que restrinja el acceso a los archivos de cada usuario, registre las actividades y otorgue privilegios especiales al administrador del sistema. Los sistemas monousuario deben emplear un software de control de acceso autorizado por el departamento de Seguridad Informática que incluya un control de arranque y un protector automático de

pantalla que se active después de un periodo de inactividad. Los computadores portátiles y de uso doméstico que contienen información de la Empresa X también están cubiertos por esta política al igual que los dispositivos de red, tales como los cortafuegos, las puertas de enlace, los enruteadores y los puentes.

Quedan prohibidos todos los comandos inter-procesadores desde sedes no pertenecientes a la Empresa X, a menos que el usuario o proceso se hayan conectado apropiadamente. Algunos ejemplos de dichos comandos son: solicitudes iniciadas remotamente para pedir una lista de usuarios conectados actualmente y una llamada de procedimiento remoto.

Los usuarios que inician sesiones a través de líneas discadas conectadas a las redes internas de la Empresa X o los sistemas de computación multiusuario deben pasar por un punto de control de acceso adicional o cortafuego antes de que aparezca el mensaje de bienvenida. Se prohíben las conexiones discadas que no pasen por cortafuegos autorizados para acceder a los sistemas conectados a la red interna de la Empresa X, salvo que el director de Seguridad Informática las autorice con antelación. Esta política se aplica para las llamadas de entrada de Internet y el intercambio de datos electrónicos.

Los puertos de mantenimiento remoto para los computadores y los sistemas de comunicación de la Empresa X deben inhabilitarse hasta que el proveedor los necesite y desactivarse de inmediato después de usarse. Las conexiones discadas pueden establecerse con los proveedores a través de llamadas salientes iniciadas por los trabajadores de la Empresa X y no se requiere un control de acceso a través de cortafuego para ninguna de las conexiones mencionadas.

Los teléfonos portátiles que usan tecnología de radio y teléfonos celulares no deben ser usados para la transmisión de datos que contengan información confidencial o secreta de la Empresa X, a menos que la

conexión esté cifrada. Otras tecnologías de redes de transmisión, tales como las redes de área local basadas en radio, no deben ser usadas para este tipo de información de la Empresa X, a menos que el enlace

esté cifrado. Tales enlaces pueden ser usados para correo electrónico siempre y cuando los usuarios entiendan que la información confidencial o secreta no debe ser transmitida usando esta tecnología.

VIRUS, GUSANOS Y CABALLOS DE TROYA

Los usuarios deben mantener activado en sus computadores el software antivirus actual autorizado, el cual puede utilizarse para rastrear todo el software proveniente de terceros y otros departamentos de la Empresa X antes de ejecutar el nuevo software y no deben omitir los procesos de rastreo que pudiesen detener la transmisión de virus.

Los usuarios tienen la responsabilidad de erradicar los virus de todos los sistemas de computadores personales bajo su control cada vez que se detecten, empleando el software instalado por el personal de la Empresa X. En cuanto el usuario detecte el virus, debe llamar al departamento de Seguridad Informática para asegurarse de que no se produzcan nuevas infecciones y de que los expertos que se necesiten para erradicar el virus se dediquen a la tarea con prontitud [aquí se puede insertar el número de teléfono].

Todo el software de los computadores personales debe copiarse antes de su uso inicial y almacenarse en un lugar seguro. Estas copias maestras no deben emplearse para las actividades normales del negocio sino más bien reservarse para la recuperación de infecciones por virus del computador, colapsos del disco duro y otros problemas e igualmente deben almacenarse en un sitio seguro.

Los computadores y las redes de la Empresa X no deben ejecutar software proveniente de fuentes distintas a los socios, grupos de usuarios expertos y confiables, autoridades conocidas en seguridad de los sistemas, proveedores de redes o computadores o proveedores de software comercial. No debe usarse el software descargado de foros o boletines electrónicos, de software compartido, de software de dominio público y otro software de fuentes no confiables, a menos que se haya sometido a pruebas rigurosas autorizadas por el departamento de Seguridad Informática.

RESPALDO DE PROGRAMAS Y DATOS

Los usuarios son responsables de efectuar el respaldo periódico de la información contenida en los computadores personales. El administrador del sistema es responsable de respaldar los sistemas de comunicación y los computadores multiusuarios. Si se solicita, el departamento de Tecnología Informática instalará o proveerá ayuda técnica para la instalación de software o hardware de respaldo.

Debe respaldarse periódicamente toda la información Secreta o Confidencial, valiosa o crítica contenida en los sistemas de computación y las redes de la Empresa X. Los gerentes de los departamentos usuarios deben definir cuál información y cuáles máquinas deben respaldarse, así como la frecuencia y el método de respaldo que se empleará, en concordancia en los siguientes lineamientos:

- Si el sistema soporta más de un usuario y contiene datos críticos para las operaciones diarias dentro de la Empresa X, se hacen respaldos diarios.

- Si el sistema se emplea para soportar funciones relacionadas con el trabajo y contiene datos críticos esenciales para las operaciones diarias de ese trabajo, se hacen respaldos semanales.
- Si el sistema se emplea principalmente como una herramienta personal y no contiene datos clasificados como de trabajo o del departamento, se hacen respaldos a discreción del usuario.

Los lapsos de tiempo mencionados anteriormente para realizar el respaldo periódico no impiden la realización de respaldos más frecuentes, según se requiera ocasionalmente por razones operativas o de negocios.

La Empresa X requiere el uso de por lo menos tres juegos de medios de almacenamiento de respaldo para ser usados alternativamente. Para los equipos multiusuario, cada vez que el software de los sistemas lo permita, los respaldos deben hacerse sin la participación del usuario final, por una red interna y fuera del horario de trabajo.

El almacenamiento de los medios de respaldo es responsabilidad del usuario del computador personal o del administrador del sistema multiusuario que participan en el proceso de respaldo. Los medios deben almacenarse en cajas fuertes a prueba de fuego en una ubicación distanciada por lo menos a varias cuadras del sistema que se está respaldando.

La información debe retenérse únicamente por el tiempo que sea necesario salvo que aparezca en la lista del Cronograma de Retención de Información de la Empresa X que se encuentra disponible en el departamento Legal, en cuyo caso debe retenérse por el periodo allí especificado. Cualquier otra información debe destruirse cuando ya no se necesite, generalmente después de dos años.

Los gerentes de departamento que definen el cronograma de respaldo también tienen la responsabilidad de preparar y actualizar regularmente los planes de contingencia de los departamentos usuarios para restaurar el servicio a todas las aplicaciones de producción, a pesar de que se requieran o no los servicios internos de red para el soporte de estas aplicaciones. El departamento de Tecnología de Información es responsable de preparar y actualizar regularmente los planes de contingencia del servicio de red. El departamento de Auditoría Interna tiene a su cargo la revisión periódica de estos planes de contingencia, incluyendo la revisión de las pruebas realizadas para validar los planes de contingencia.

Toda la información Secreta o Confidencial almacenada en los medios de respaldo debe cifrarse empleando métodos autorizados.

CIFRADO

Cuando la información Secreta o Confidencial de la Empresa X se transmite a través de cualquier red de comunicación, debe enviarse en forma cifrada. Cada vez que el código fuente de la Empresa X o el código fuente que le ha sido confiado por un socio de negocios debe enviarse por una red, debe igualmente estar cifrado. Las definiciones de las palabras "Confidencial" y "Secreta" se pueden encontrar en la Política de Clasificación de Datos [aquí se puede insertar un enlace intranet a esa política].

Cuando la información Confidencial o Secreta no se está usando, debe almacenarse en forma cifrada, lo cual significa que cuando se almacena o se transporta en medios de almacenamiento legibles, debe cifrarse.

El cifrado de información almacenada o en tránsito debe completarse mediante el uso de productos disponibles comercialmente y autorizados por el departamento de Seguridad Informática.

Cada vez que se emplee el cifrado, los trabajadores no deben eliminar la única versión legible de la información a menos que hayan demostrado que el proceso de descifrado es capaz de restablecer una versión legible de la información.

Las claves de cifrado usados para la información de la Empresa X siempre se clasifican como información Confidencial o Secreta. El acceso a dichas claves debe limitarse a aquellas personas con necesidad de conocer. A menos que se obtenga la autorización del gerente de Seguridad Informática, las claves de cifrado no deben revelarse a los consultores, a los contratistas, al personal temporal o a otros terceros y deben estar siempre cifradas cuando se envían a través de una red.

Cada vez que dichas facilidades se encuentren disponibles comercialmente, la Empresa X debe emplear procesos automatizados en lugar de procesos manuales en el manejo de las claves de cifrado para la protección de la información en las redes de la Empresa X.

COMPUTADORES PORTÁTILES

Los trabajadores que posean computadores portátiles o de mano que contengan información Confidencial de la Empresa X no deben descuidar sus equipos en ningún momento a menos que su información esté cifrada.

Los trabajadores que tengan computadores portátiles que contengan información Confidencial o Secreta no cifrada de la Empresa X no deben dejar sus computa-

dores como equipaje en aerolíneas o con porteros en cualquier hotel, sino mantenerlos consigo como equipaje de mano.

Cada vez que información Confidencial o Secreta se guarde en disco flexible, cinta magnética, tarjeta inteligente u otro medio de almacenamiento, el medio debe estar identificado apropiadamente con la clasifi-

cación de confidencialidad más alta correspondiente. Cuando no se estén usando, estos medios deben almacenarse en una caja fuerte, en mobiliario cerrado con llave y otros lugares similares. Se puede encontrar

información adicional en la Política de Seguridad Informática de Teletrabajo [aquí se puede insertar un enlace intranet].

IMPRESIÓN REMOTA

Las impresoras no deben desatenderse cuando se está imprimiendo o se va a imprimir información Confidencial o Secreta y las personas a cargo de ellas deben estar autorizadas para tales efectos. Está permitido que la

impresión se haga sin supervisión cuando el área alrededor de la impresora está físicamente protegida de forma que personas no autorizadas para ver el material no tengan acceso a la misma.

PRIVACIDAD

Salvo que acuerdos contractuales establezcan lo contrario, los mensajes que se envían a través de los sistemas de comunicación y los computadores de la Empresa X son propiedad de la Empresa X, por lo cual la gerencia se reserva el derecho de examinar todos los datos almacenados o transmitidos por estos sistemas. Debido a que los sistemas de comunicación y los computadores de la Empresa X deben usarse únicamente para propósitos empresariales, los trabajadores no deben aspirar a tener privacidad en relación con la información que se almacene o envíe a través de estos sistemas.

Cuando proporciona servicios de red, la Empresa X no suministra servicios de protección de mensajes de manera predeterminada, como por ejemplo el cifrado;

no asume ninguna responsabilidad por la divulgación de la información enviada a través de las redes ni garantiza la privacidad de la información manejada por las redes internas de la Empresa X. En los casos en que se requiera el cifrado de la sesión u otros controles especiales, el usuario es responsable de garantizar que se tomen medidas de seguridad adecuadas. Ninguno de los enunciados de este párrafo debe interpretarse de manera tal que se entienda que la política de la Empresa X no respalda los controles estipulados en los acuerdos con terceros, como por ejemplo las organizaciones que han confiado su información confidencial a la Empresa X.

REGISTROS Y OTRAS HERRAMIENTAS DE SEGURIDAD EN SISTEMAS

Todo sistema de comunicaciones o de computación multiusuario debe incluir suficientes herramientas automatizadas para ayudar al administrador del sistema a verificar el estado de la seguridad del mismo, como por ejemplo mecanismos para el registro, detección y corrección de problemas de seguridad comúnmente encontrados.

Cuando los costos sean justificables, estas herramientas automatizadas deben usarse en las redes y los computadores de la Empresa X. Por ejemplo, debe usarse con regularidad un software que verifique en forma automática las licencias del software de los computadores personales a través de una red de área local.

Hasta donde el software lo permita, los sistemas de comunicaciones y de computación que manejan información confidencial, valiosa o crítica deben registrar correctamente todos los eventos significativos

en materia de seguridad, como por ejemplo los cambios de identificador de usuario durante una sesión en línea, los intentos por descifrar contraseñas, los intentos de usar privilegios no autorizados, las modificaciones a las aplicaciones de producción, las modificaciones del software del sistema, los cambios en los privilegios del usuario y en las configuraciones del sistema de registro.

Los registros que contienen sucesos de seguridad significativos en los computadores o sistema de comunicaciones deben retenerse por un periodo mínimo de tres meses durante el cual los registros deben guardarse de manera tal que no puedan modificarse y únicamente las personas autorizadas puedan leerlos.

Cuando se sospeche que se ha cometido un delito o un abuso relacionado con algún computador o la red, la información pertinente debe capturarse y almacenarse adecuadamente fuera de línea hasta que se determine

que la Empresa X no tomará acciones legales o usará la información de alguna otra manera. La información que debe recogerse de inmediato incluye los registros del sistema, pistas para la auditoría de las aplicaciones, otros indicios de los estados actuales del sistema y copias de todos los archivos relacionados.

El personal de operaciones de computación, de seguridad informática o de administración de sistemas, debe revisar periódica y oportunamente todos los registros que reflejen sucesos significativos en materia de seguridad.

Los usuarios deben ser informados de los actos específicos que constituyen violaciones en la seguridad de los computadores y las redes y de que dichas violaciones serán registradas.

Aunque no es necesario que los administradores del sistema carguen con prontitud la versión más reciente de los sistemas operativos, sí tienen que aplicar todos los parches de seguridad a los sistemas operativos que han sido dados a conocer por grupos de usuarios expertos y confiables, autoridades conocidas en seguridad de los sistemas o el proveedor del sistema operativo. En los computadores y las redes de la Empresa X, solamente pueden usarse las herramientas de seguridad suministradas por estas fuentes o por organizaciones comerciales de software.

MANEJO DE LA INFORMACIÓN DE SEGURIDAD DE LA RED

Cada cierto tiempo, el director de Seguridad Informática designará a personas para auditar el cumplimiento de ésta y las otras políticas relacionadas con la seguridad de la red y de los computadores. Igualmente, todo trabajador debe reportar con prontitud al gerente de Seguridad Física cualquier sospecha de problemas en la seguridad de la red, incluyendo intromisiones y situaciones de incumplimiento.

Siempre y cuando no hubiere habido intención de dañar los sistemas de la Empresa X, no se tomarán acciones disciplinarias si los trabajadores reportan una infección por virus de un computador inmediatamente después de haberlo notado, aun cuando haya habido negligencia de su parte.

Todas las fallas en el funcionamiento del software de sistemas o de la red deben reportarse inmediatamente al departamento de Tecnología de Información o al proveedor externo de servicio de sistemas informáticos.

La información sobre las medidas de seguridad para los sistemas de comunicación y los computadores de la Empresa X es confidencial y no debe ser revelada a personas que no sean usuarios autorizados de los sistemas mencionados, a menos que se haya obtenido el permiso del departamento de Seguridad Informática. Está prohibida la publicación de números telefónicos de modem o alguna otra información sobre el acceso al sistema; sin embargo, la divulgación de las direcciones de correo electrónico de Internet está permitida.

SEGURIDAD FÍSICA DE LOS EQUIPOS DE COMPUTACIÓN Y DE COMUNICACIONES

Todo equipo de red de la Empresa X ubicado en una oficina abierta, así como los equipos de computación ubicados en oficinas de servicio de ventas, deben asegurarse físicamente con dispositivos antirrobo. Además deben usarse controles adicionales de acceso físico, por ejemplo, los servidores de red de área local deben colocarse en gabinetes, armarios o salas de computación cerrados.

El acceso a las oficinas del personal de desarrollo de sistemas, a los armarios con cableado de teléfono, a las salas de computadores, a las salas de comunicaciones y otras áreas de trabajo en donde se maneje información

Confidencial o Secreta debe restringirse físicamente. La gerencia responsable por el personal que trabaja en estas áreas debe consultar al departamento de Seguridad Informática para determinar el método adecuado de control de acceso.

Todos los trabajadores que deban guardar información Confidencial o Secreta en sus casas para realizar su trabajo deben recibir mobiliario con cerraduras para el adecuado almacenamiento de esta información. Al momento de dejar de prestar sus servicios a la Empresa X, tanto el mobiliario como la información allí almacenada deben devolverse de inmediato.

La información Confidencial o Secreta no debe descargarse a ubicaciones remotas tales como las oficinas de ventas, a menos que se instalen y se cumplan a cabalidad las medidas apropiadas de seguridad física y las facilidades de cifrado.

EXCEPCIONES

El gerente de Seguridad Informática reconoce que en circunstancias poco usuales, algunos trabajadores necesitarán emplear sistemas que no estén conformes

con estas políticas. Todos esos casos deben ser autorizados por escrito y con antelación por el gerente de Seguridad Informática.

VIOLACIONES

Todo trabajador de la Empresa X que por voluntad propia y deliberada viole esta política, estará sujeto a acciones disciplinarias, incluyendo el cese de la relación laboral.

GLOSARIO

Administrador del sistema: Persona designada que tiene privilegios especiales sobre sistemas de computadores multiusuario y que vela por la seguridad del mismo y otros asuntos administrativos.

Agentes: Tipo novedoso de software que realiza tareas especiales en favor del usuario, tales como la búsqueda en múltiples bases de datos de la información designada.

Algoritmo: Proceso matemático utilizado para efectuar determinados cálculos. En el campo de la seguridad informática, por lo general, se emplea para referirse al proceso de realización de cifrados.

Ataque mediante deducción de contraseñas: Proceso computarizado o manual mediante el cual se suministran varias contraseñas posibles a un computador, en un intento por obtener un acceso no autorizado.

Cifrado: Proceso que incluye la codificación de datos, con el objeto de lograr confidencialidad, anonimato, marca de hora y fecha (time stamping) y demás objetivos de seguridad.

Clave de cifrado: Clave secreta o cadena de bits que se utiliza para controlar el algoritmo que rige un proceso de cifrado.

Computador independiente: Computador que no se encuentra conectado a una red o a cualquier otro computador, por ejemplo, un computador personal independiente.

Contraseña: Cualquier sucesión secreta de caracteres que se utilizan para identificar de manera positiva al usuario o proceso computarizado.

Contraseña compartida: Contraseña conocida o utilizada por más de una persona.

Contraseña dinámica: Contraseña que es modificada cada vez que el usuario ingresa al sistema de un computador.

Contraseña predeterminada: Contraseña inicial que se emite cuando se crea el identificador de un nuevo usuario, o contraseña inicial que suministra el proveedor, al momento de entregar el hardware o el software.

Control de Acceso: Sistema utilizado para restringir las actividades de los usuarios y los procesos de acuerdo con la necesidad de conocer.

Control de acceso basado en contraseñas: Software que depende de las contraseñas como mecanismo primario para controlar los privilegios en el sistema.

Copias maestras del software: Copias del software que se encuentran retenidas en un archivo y que no son utilizadas para las actividades comerciales normales.

Cortafuego: Barrera lógica que evita que los usuarios de computadores o procesos computarizados vayan más allá de un punto determinado de la red, salvo que estos usuarios o procesos hayan pasado por cierta verificación de seguridad, tal como suministrar una contraseña.

Cronograma de retención informática: Listado formal de los tipos de información que se deben retener con fines de archivo y los períodos de tiempo que deben guardarse.

Declaración de conformidad: Documento utilizado para obtener del usuario de computadores un compromiso en el cual dicho usuario se apega a las políticas y procedimientos del sistema.

Enrutador: Dispositivo que interconecta las redes utilizando distintos estratos del Modelo de Referencia de Interconexión de Sistemas Abiertos (Open Systems Interconnection (OSI)).

Identificación positiva: El proceso de establecer la identidad definitiva de un usuario de computadores.

Identificador de usuario: Se conoce también como cuentas; son sucesiones de caracteres que asignan una identificación particular a los usuarios de computadores o procesos computarizados.

Identificador de usuario privilegiado: Identificador de aquel usuario a quien le ha sido otorgada la facultad de realizar actividades especiales, tal como apagar un sistema multiusuario.

Información sensible: Designación de información cuya divulgación irá en detrimento de la Empresa X o de sus afiliados comerciales.

Información secreta: Información particularmente sensible cuya divulgación significa pérdida para la Empresa X o de sus afiliados comerciales.

Información crítica: Cualquier información esencial para las actividades comerciales de la Empresa X, y cuya destrucción, modificación y falta de disponibilidad ocasionarían una grave interrupción de las mismas.

Información confidencial: Cualquier información cuya divulgación puede ir en detrimento de la Empresa X o de sus afiliados comerciales.

Información valiosa: Información que tiene para la Empresa X u otra parte un valor financiero significativo.

Lector de Distintivos: Dispositivo que lee los distintivos de identificación del trabajador y se interconecta con el sistema de control de acceso físico que controlan las puertas que se encuentran aseguradas.

Macro: Secuencia de comandos procedimentales programable por el usuario final, con el propósito de lograr un determinado resultado.

Mensaje de bienvenida: Mensaje inicial que se le presenta a un usuario cuando se conecta con un computador.

Parche de Seguridad: Software que se utiliza para resolver problemas de seguridad, o de otro tipo, que se aplica comúnmente a los sistemas operativos, sistemas de administración de bases de datos y otros.

Permiso predeterminado para acceder a un archivo: Privilegios de control de acceso que se asignan a los usuarios de computadores para leer, escribir, ejecutar y borrar un archivo, sin la participación de un administrador o de dispositivos de seguridad.

Privilegio: Facultad concedida para realizar ciertas acciones en un computador, tal como leer un archivo específico del computador.

Protector de pantalla: Programa de computador que blanquea automáticamente la pantalla del monitor de un computador, luego de un determinado periodo de inactividad.

Procesador de interface: Computador pequeño que se utiliza para el manejo de la interfase de comunicaciones de otro computador.

Proceso de Inicio (y sus derivados): Proceso de iniciación de un sistema de computadores, desde el momento en que éste se encuentra apagado o desconectado.

Puente: Dispositivo que interconecta las redes o que de algún modo permite la conexión de los circuitos de las redes.

Puerta de enlace: Sistema computarizado utilizado para conectar redes y que puede restringir el flujo de información y emplea algunos métodos de control de acceso.

Privilegio especial en el sistema: Privilegios de acceso al sistema que permiten al usuario o proceso involucrado realizar actividades que normalmente no son otorgados a otros usuarios.

Reinicialización de contraseña: Asignación de una contraseña temporal a aquel usuario que olvida o extravía su contraseña.

Requerimiento y respuesta: Proceso que se utiliza para identificar a los usuarios de computadores, el cual incluye la emisión aleatoria de un requerimiento a una

estación de trabajo remota que luego es transformado, mediante el uso de un proceso de cifrado, y se envía de vuelta como respuesta al computador que está conectado.

Resumen de comandos de inicio de sesión: Conjunto de comandos almacenados que permiten a un usuario acceder al sistema de un computador en forma automática.

Sistema de computadores multiusuario: Cualquier computador que pueda soportar a más de un usuario simultáneamente.

Software antivirus: Software disponible a nivel comercial que busca ciertos patrones de bits u otras evidencias de infección de virus en un computador.

Suspensión del identificador de usuario: Proceso de revocar los privilegios asociados con un identificador de usuario.

Tarjetas portátiles: Sistema comercial de contraseñas dinámicas que utiliza una tarjeta inteligente para generar contraseñas que serán utilizadas una sola vez, siendo éstas distintas para cada sesión.

Teclas de función: Teclas especiales de un teclado que pueden ser definidas por un usuario para que realice ciertas actividades, tales como guardar un archivo.

Técnica extendida de autenticación de usuario: Cualquiera de los diversos procesos que se utilizan para reforzar el proceso de identificación de un usuario, lo cual normalmente se logra mediante identificadores de usuario y contraseñas fijas, tales como las tarjetas portátiles (hand-held tokens) y las contraseñas dinámicas.

Usuario final: Usuario que emplea los computadores para apoyar las actividades comerciales de la Empresa X y que actúa como fuente o destino de la información que fluye a través de un sistema de computadores.

Verificación de condición de seguridad: Proceso mediante el cual se garantiza que los controles están instalados y funcionan correctamente.



Capítulo 11 MODELO DE POLÍTICA DE SEGURIDAD EN INTERNET PARA USUARIOS

INTRODUCCIÓN

Oportunidades y Riesgos—La amplia variedad de nuevos recursos, servicios e interconectividad disponibles a través de la Internet plantean nuevas oportunidades de negocio, así como nuevos riesgos en materia de seguridad y privacidad. La política oficial de la Empresa X aquí descrita en relación con la seguridad en Internet, es una respuesta a estos riesgos.

Aplicabilidad—Esta política se aplica a todos los trabajadores, empleados, contratistas, consultores, personal temporal y voluntarios que usan la Internet con los recursos computacionales y de redes de la Empresa X y a los usuarios que de algún modo se conectan con la Empresa X. Se espera que todos estos usuarios estén familiarizados con esta política y la cumplan en su totalidad. Las preguntas sobre la política deben ser dirigidas al coordinador de Seguridad Informática del departamento del usuario o al gerente corporativo de Seguridad Informática. Las violaciones a esta política

pueden conducir a la revocatoria de privilegios en el sistema o a acciones disciplinarias adicionales, incluyendo el cese de la relación laboral.

Autorización Previa de la Gerencia—El acceso a Internet, aparte del correo electrónico, será otorgado solamente a aquellos trabajadores que tienen una necesidad justificada por razones empresariales. La capacidad de acceder y de participar en otras actividades de Internet no es un incentivo al cual todos los trabajadores tienen derecho. Si un trabajador no tiene suficiente acceso a la Internet, pero lo necesita para un proyecto en particular, puede usar los sistemas especiales compartidos que se encuentran en la biblioteca corporativa. Para recibir privilegios de acceso a Internet, todos los trabajadores deben completar y aprobar el curso de adiestramiento de seguridad informática asistido por computadores.

INTEGRIDAD DE LA INFORMACIÓN

Confiabilidad de la Información—Toda la información adquirida de Internet debe considerarse no confiable hasta que se confirme con información proveniente de otra fuente. Antes de emplear información suministrada gratuitamente por Internet para la toma de decisiones empresariales, los trabajadores deben corroborar la información consultando otras fuentes.

Verificación Antivirus—Todos los archivos no texto descargados de Internet y provenientes de fuentes que no pertenecen a la Empresa X deben ser examinados con software antivirus antes de usarlos. Cuando el proveedor externo del software no es confiable, el software descargado debe probarse en una máquina independiente, no empleada para la producción, que haya sido respaldada recientemente. Los archivos descargados deben descifrarse y descomprimirse antes de ser sometidos a la verificación antivirus. Es recomendable el uso de firmas digitales para verificar

que un archivo no ha sido modificado por partes no autorizadas, mas no garantiza que el archivo esté libre de virus, caballos de Troya y otros problemas.

Descarga de Software—La Empresa X ha implementado un sistema automático de distribución de software para instalar el software autorizado más reciente en sus computadores. Para rastrear en forma automática todo el software que reside en estos mismos sistemas, se utiliza un sistema distinto. Como ya se ha explicado en la Política de Seguridad de Computadores Personales, los trabajadores no deben instalar software en los computadores suministrados por la Empresa X, bien sea que se hayan descargado de la Internet o se hayan obtenido de otro modo.

Tecnología de Actualización Automática—Queda prohibida la actualización automática de software o de información en los computadores de la Empresa X a través de tecnología de actualización automática de

Internet, a menos que el sistema del proveedor haya sido probado y autorizado por el grupo de Internet dentro del departamento de Sistemas Informáticos.

Confirmación de Identidad—Antes de que los trabajadores revelen cualquier información interna de la Empresa X, celebren contratos o hagan pedidos de productos a través de redes públicas, debe confirmarse la identidad de las personas y las organizaciones contactadas. Lo ideal es hacerlo mediante firmas o certificados digitales; sin embargo, cuando éstos no estén disponibles, pueden emplearse cartas de crédito, referencias de terceros y conversaciones telefónicas.

Anonimato del usuario—Queda prohibido falsear, ocultar o sustituir la identidad de un usuario en Internet o en cualquier sistema de comunicaciones electrónicas de la Empresa X. El nombre del usuario, la dirección de correo electrónico, la afiliación a la organización y otros detalles incluidos en los mensajes o transcripciones deben señalar al verdadero autor de los mismos. Si los usuarios tienen necesidad de emplear redespachadores de correo y otras facilidades anónimas, deben hacerlo en su tiempo libre, con sus propios sistemas informáticos y cuentas de proveedores de servicio de Internet. Se permite el uso de conexiones anónimas FTP, UUCP,

HTTP o exploración de la web y otros métodos de acceso establecidos donde se supone que los usuarios son anónimos.

Archivos anexos al correo electrónico—Los trabajadores deben abstenerse de abrir los archivos adjuntos a su correo electrónico salvo que provengan de un remitente confiable. Cuando los trabajadores reciban archivos adjuntos de remitentes conocidos y confiables, deben usar un paquete antivirus antes de abrirlos.

Cambios a páginas web—Los trabajadores no deben establecer nuevas páginas de Internet o realizar modificaciones en las páginas existentes relacionadas con el negocio de la Empresa X, a menos que obtengan una autorización del comité gerencial de Internet. Los cambios incluyen añadir enlaces a otros sitios, actualizar la información presentada y alterar la diagramación de una página. Este comité debe garantizar que todo el material publicado tenga una apariencia coherente e impecable, esté alineado con los objetivos empresariales y esté protegido con medidas adecuadas de seguridad.

Archivos de Páginas Web—Cada versión del sitio de Internet y del sitio de comercio de la Empresa X debe resguardarse en dos ubicaciones físicamente separadas. El comité gerencial de Internet designará un administrador web para guardar este respaldo y suministrar copias de las páginas históricas a solicitud.

CONFIDENCIALIDAD DE LA INFORMACIÓN

Intercambio de Información—El software, la documentación y toda la información interna de la Empresa X no debe venderse ni transferirse de algún otro modo a ningún tercero que no pertenezca a la Empresa X para ningún propósito distinto a los propósitos de negocio expresamente autorizados por la gerencia. El intercambio de software o de datos entre la Empresa X y cualquier tercero no debe proceder, a menos que se haya suscrito un acuerdo por escrito que especifique los términos del intercambio y la manera en que el software o los datos se van a manejar y proteger. Las prácticas empresariales normales, tales como el envío de un producto en respuesta a una orden de compra del cliente, no requieren de un acuerdo específico ya que las condiciones y términos están implícitos.

Exposición de Materiales—Los trabajadores no deben colocar material no cifrado de la Empresa X en ningún computador accesible públicamente por la Internet que soporte FTP anónimos o servicios similares, a menos que la exposición de estos materiales haya sido autorizada por el director de Relaciones Públicas. La

información interna de la Empresa X no debe colocarse en ningún computador, a menos que las personas que tienen acceso al mismo tengan una necesidad justificada por razones de negocios para conocer dicha información.

Interceptación de Mensajes—La información secreta, privada o propiedad de la Empresa X no debe enviarse por Internet, a menos que haya sido cifrada con métodos autorizados. Salvo que se sepa que es del dominio público, el código fuente siempre debe cifrarse antes de enviarlo por Internet. Por las mismas razones, los servicios de teléfono de Internet no deben emplearse para los negocios de la Empresa X a menos que se sepa que la conexión esté cifrada.

Parámetros de Seguridad—A menos que se sepa que la conexión está cifrada, los números de tarjetas de crédito, los números de tarjetas de llamadas telefónicas, las contraseñas de acceso fijas y otros parámetros de seguridad que puedan emplearse para obtener acceso a bienes y servicios, no deben enviarse por Internet en

forma legible. Los procesos de cifrado están permitidos si están autorizados por el gerente corporativo de Seguridad Informática.

REPRESENTACIONES PUBLICAS

Representaciones Externas—Los trabajadores pueden indicar su afiliación con la Empresa X en listas de direcciones de correo, sesiones de chat y otras ofertas en la Internet, bien sea añadiendo algunas palabras explícitamente o, implícitamente, a través de una dirección de correo electrónico. En cualquiera de los casos, cuando los trabajadores indiquen una afiliación, también deben señalar con claridad que las opiniones expresadas son a título personal y no necesariamente las de la Empresa X, a menos que ellos hayan sido expresamente designados como voceros de ésta última. Si se indica afiliación con la Empresa X, se prohíben las declaraciones en defensa de intereses políticos y la promoción de productos o servicios a menos que hayan sido autorizadas previamente por el director de Relaciones Públicas. A excepción de las actividades normales de mercadeo y de servicios al cliente, todas las representaciones en nombre de la Empresa X deben estar autorizadas por el director de Relaciones Públicas.

Conducta Apropiada—Siempre que se incluya la afiliación con la Empresa X en un mensaje o publicación en Internet, se prohíben terminantemente los ataques escritos, como amenazar a otro usuario o a otra organización a través de Internet, así como todos los mensajes cuya intención sea acosar, molestar o alarma a otra persona.

Eliminación de Mensajes—Los mensajes enviados a los grupos de discusión, a boletines electrónicos y a otros foros públicos de la Internet que incluyan una afiliación implícita o explícita con la Empresa X, pueden eliminarse si la gerencia considera que los mismos no se consideran acordes con los intereses del negocio o con la política vigente de la Empresa X. Se incluyen en esta categoría las declaraciones políticas y religiosas, el uso de lenguaje grosero o soez y otras afirmaciones consideradas como hostigamiento a otras personas basándose en la raza, el credo, el color, la edad, el sexo, las discapacidades físicas o las preferen-

cias sexuales. La decisión de eliminar el correo electrónico debe tomarla el gerente corporativo de Seguridad Informática o el director de Recursos Humanos. Cuando sea práctico y viable, los individuos responsables del mensaje serán informados de la decisión y tendrán la oportunidad de eliminar el mensaje ellos mismos.

Divulgación de Información Interna—Los trabajadores no deben divulgar públicamente información interna de la Empresa X a través de la Internet que pueda afectar negativamente el precio de las acciones, las relaciones con los clientes o la imagen pública de la Empresa X, a menos que hayan obtenido la autorización del director de Relaciones Públicas o de un integrante del equipo de alta gerencia. Esta información abarca las posibilidades de negocio, los productos que están en investigación y desarrollo, los análisis de rendimiento de los productos, las fechas de lanzamiento de los mismos y problemas internos de los sistemas de información. Quedan eximidas de esta política las respuestas a mensajes de correo electrónico de un cliente específico.

Divulgación Involuntaria—Debe tenerse mucho cuidado en formular adecuadamente los comentarios y las preguntas que se envían a las listas de direcciones, los grupos públicos de noticias, Usenet y otros destinos públicos en la Internet. Antes de enviar cualquier material, los trabajadores deben considerar si el mensaje pudiese colocar a la Empresa X en desventaja competitiva significativa o si el material pudiese ocasionar problemas de relaciones públicas. Los trabajadores deben tener presente que un competidor puede reconstruir varios fragmentos separados de información para formar un cuadro que revele información confidencial, la cual pudiese ser usada posteriormente en contra de la Empresa X. Los trabajadores nunca deben colocar en Internet los productos específicos de red o de computación que emplea la Empresa X.

DERECHOS SOBRE LA PROPIEDAD INTELECTUAL

Derechos Reservados—Se prohíbe el copiado de software que no se realice conforme a la licencia del proveedor cuando el trabajador esté en su lugar de trabajo o cuando se estén empleando recursos de

computación o de redes de la Empresa X, al igual que la participación en boletines de anuncios de software pirata y actividades similares fuera del horario de trabajo, debido a que crean un conflicto de intereses con

el trabajo en la Empresa X. La reproducción, el reenvío o cualquier otro modo de republicación o redistribución de palabras, gráficos o cualquier otro material con derechos reservados debe hacerse solamente con el permiso del autor o Propietario. Del mismo modo, los trabajadores deben asumir que todos los materiales en la Internet tienen derechos reservados a menos que un aviso específico indique lo contrario. Cuando la información proveniente de la Internet se incorpore en informes internos o se use para otros fines, todo el

material debe incluir etiquetas tales como "copyright, todos los derechos reservados" además de detalles sobre la fuente de la información.

Directorios Modificables Públicamente—Todos los directorios modificables públicamente en los computadores de la Empresa X conectados a la Internet deben revisarse y limpiarse al final de cada día. Los trabajadores que usen los computadores de la Empresa X no deben involucrarse en el intercambio de software pirata, contraseñas hurtadas, números de tarjetas de crédito robadas y material gráfico o escrito inapropiado.

CONTROL DE ACCESO

Autentificación de Usuario Entrante—Todos los usuarios que deseen establecer una conexión en tiempo real con los computadores internos de la Empresa X a través de la Internet deben emplear un producto de red privada virtual (VPN, por sus siglas en inglés) autorizado por el departamento de Seguridad Informática el cual puede cifrar todo el tráfico que se intercambia. Estos productos VPN también deben autenticar usuarios remotos en un cortafuego antes de permitirles el acceso a la red interna de la Empresa X. Este proceso de autentificación debe completarse mediante un sistema de contraseña dinámica autorizado por el gerente corporativo de Seguridad Informática. Algunos ejemplos de tecnología autorizada incluyen tarjetas inteligentes portátiles con contraseñas dinámicas y sistemas de requerimiento y respuesta que sean transparentes para el usuario. Los sistemas públicos designados no requieren de procesos de autentificación de usuario porque se supone que las interacciones son anónimas.

Seguridad Remota del Equipo—Los trabajadores que no hayan instalado las mejoras o los parches requeridos al software o cuyos sistemas estén infectados por virus deben desconectarse automáticamente de la red de la Empresa X hasta que se restablezca un ambiente seguro de computación. Los computadores usados por todos los trabajadores que empleen tecnología VPN deben ser rastreados remotamente en forma automática para determinar si el software está actualizado y si el sistema ha sido protegido adecuadamente.

Restricción de Acceso de Terceros—No deben otorgarse privilegios entrantes de acceso a la Internet a terceros, incluyendo proveedores, contratistas, consultores, personal temporal o personal de organizaciones externas u otros terceros a menos que el gerente del sistema en cuestión determine que estos individuos

tienen una necesidad justificada de negocios para dicho acceso. Estos privilegios deben habilitarse únicamente para ciertos individuos y sólo por el periodo de tiempo requerido para completar las tareas autorizadas.

Autentificación de Usuario de Explorador—Los trabajadores no deben guardar contraseñas fijas en sus exploradores web o en sus clientes de correo electrónico. Estas contraseñas fijas deben ser suministradas cada vez que se invoca un explorador o un cliente de correo electrónico. Las contraseñas de explorador pueden ser guardadas cuando debe suministrarse una contraseña de arranque cada vez que se enciende el computador y cuando se solicita una contraseña de protector de pantalla cada vez que el sistema permanece inactivo por un periodo específico de tiempo. Los usuarios de los computadores de la Empresa X deben rechazar todos los ofrecimientos del software de colocar cookies en su computador para que puedan conectarse en forma automática la próxima vez que visiten un sitio particular de la Internet. Los cookies que sirven para otros propósitos están permitidos.

Agrupadores de Datos—Los trabajadores no deben suministrar sus identificadores de usuario de la Internet y las contraseñas a agrupadores de datos, a servicios de resumen de datos y de formato ni a ningún otro tercero.

Proveedores de Servicio de Internet—A excepción de los teletrabajadores y de los usuarios de computadores móviles, los trabajadores no deben emplear cuentas de proveedores de servicio de Internet y líneas de discado para acceder a Internet con los computadores de la Empresa X. Toda la actividad en Internet debe atravesar los cortafuegos de la Empresa X para que se puedan aplicar los controles de acceso y los demás mecanismos de seguridad. Los usuarios deben emplear la dirección de correo electrónico de la Empresa X para el correo

electrónico de Internet. Queda prohibido el uso de la dirección personal de correo electrónico para este propósito.

Establecimiento de Conexiones de Red—A menos que se haya obtenido la autorización previa del gerente de Servicios de Telecomunicaciones, los trabajadores no deben establecer conexiones de Internet o de otras redes externas que pudiesen permitir que usuarios no pertenecientes a la Empresa X obtengan acceso a los sistemas y a la información de la Empresa X. Estas conexiones incluyen el establecimiento de sistemas de archivo multicomputador, páginas de Internet, sistemas de comercio en Internet y servidores FTP.

Establecimiento de Nuevos Canales de Negocios—A menos que el vicepresidente de Sistemas de Información, el vicepresidente de Mercadeo y el asesor

legal principal lo hayan autorizado previamente, los trabajadores no deben usar conexiones nuevas o existentes de Internet para establecer nuevos canales de negocios. Estos canales incluyen acuerdos para el intercambio de datos electrónicos, centros comerciales electrónicos con compras en línea y servicios de base de datos en línea.

Realización de negocios a través de Internet—A menos que se haya obtenido una autorización previa del departamento de Compras, los trabajadores de la Empresa X no deben comprar ningún bien o servicio a través de la Internet cuando éstos son ofrecidos por un negocio establecido o con operaciones en un país extranjero.

USO PERSONAL

Uso Personal—Los trabajadores con acceso a Internet y que deseen explorarla para propósitos personales, incluyendo juegos, grupos de noticias y otras actividades no relacionadas con el negocio, deben hacerlo durante su tiempo libre y no en horas hábiles. El uso de los recursos de computación de la Empresa X para propósitos personales se permite siempre y cuando el aumento en el costo por dicho uso sea insignificante, no tenga prioridad sobre las actividades de negocio de la Empresa X y no conlleve la creación de un ambiente de trabajo desfavorable o un ejemplo de conducta deficiente. Los trabajadores no deben emplear Internet u otros sistemas internos de información de forma tal que afecte la productividad de otros trabajadores. Algunos ejemplos son las cartas en cadena y la difusión de peticiones de dinero para obras de caridad. Los recursos de computación de la Empresa X no deben revenderse a otras partes ni tampoco emplearse para propósitos personales de negocio, como por ejemplo, ofrecer consultoría fuera del horario de trabajo.

Sitios Ofensivos de la Web—La Empresa X no es responsable del contenido en los sitios de la web. Cuando los usuarios de los computadores de la Empresa X usan la Internet y se dan cuenta de que se han conectado con sitios que tienen un contenido censurable, como por ejemplo material violento, sexista, racista o sexualmente explícito o potencialmente ofensivo, deben desconectarse del sitio de inmediato.

Bloqueo de Sitios y Tipos de Contenido—La posibilidad de conectarse con un sitio específico de la web no implica que se permita que los usuarios de los sistemas de la Empresa X visiten ese sitio. De hecho, ésta puede, a discreción, restringir o bloquear la descarga de ciertos tipos de archivo que pudiesen ocasionar una distorsión en el servicio de la red, incluyendo los archivos gráficos y de música

EXPECTATIVAS DE PRIVACIDAD

Sin Protección Pre-establecida—Los trabajadores que usen los sistemas de información de la Empresa X o Internet deben tener presente que sus comunicaciones no están automáticamente protegidas de ser vistas por terceros. Salvo que se utilice el cifrado, los trabajadores no deben enviar información a través de Internet si consideran que es confidencial o privada.

Revisión de la Gerencia—En cualquier momento y sin previo aviso, la gerencia de la Empresa X se reserva el derecho de examinar los mensajes de correo electrónico, los archivos en los computadores personales, los archivos caché del explorador de la web, los marcadores del buscador de la web, los registros de los sitios de la web visitados, las configuraciones del sistema de

computación y cualquier otra información que se almacene o que pase a través de los computadores de la Empresa X.

Registros—La Empresa X registra rutinariamente los sitios visitados en la web, los archivos descargados, el tiempo conectado a Internet e información relacionada. Los gerentes de departamento reciben informes de dicha información y la usan para determinar los tipos de uso de Internet que son apropiados para las actividades de negocio del departamento.

Correo Electrónico No Deseado—Los usuarios no deben utilizar los sistemas de computación de la Empresa X para transmitir anuncios por correo

electrónico o mensajes comerciales no solicitados que puedan provocar quejas por parte de los destinatarios. Estos mensajes prohibidos incluyen una amplia variedad de promociones y peticiones no solicitadas tales como cartas en cadena, planes de pirámide y discursitos de mercadeo directo. Cuando los trabajadores reciban correo electrónico no deseado y no solicitado, deben abstenerse de responder directamente al remitente y reenviar el mensaje al administrador de correo electrónico en la Empresa X quien podrá tomar las medidas necesarias para impedir transmisiones posteriores

REPORTES DE PROBLEMAS DE SEGURIDAD

Proceso de Notificación—Si la información confidencial de la Empresa X se pierde, se divulga a partes no autorizadas o se tiene sospecha de cualquiera de las situaciones anteriores, debe notificarse al gerente de Seguridad Informática de inmediato. Si ha ocurrido cualquier uso no autorizado de los sistemas de información de la Empresa X o se sospecha que está ocurriendo, debe notificarse al gerente corporativo de Seguridad Informática con prontitud. Cada vez que las contraseñas u otros mecanismos de control de acceso al sistema se pierden, son robadas o reveladas o existe sospecha de cualquiera de las situaciones anteriores, debe informarse al gerente corporativo de Seguridad Informática inmediatamente. Cualquier comportamiento inusual de los sistemas, como por ejemplo el extravío de archivos, los colapsos frecuentes del sistema y los mensajes enviados equivocadamente, deben ser reportados de inmediato a la mesa de ayuda. Los detalles de los problemas de seguridad no deben discutirse abiertamente sino compartirse basándose en la necesidad de conocer.

Reportes Falsos de Seguridad—Los trabajadores que reciban información sobre aspectos vulnerables del sistema deben reenviarla al gerente corporativo de Seguridad informática, quien determinará las acciones apropiadas a tomar. Los trabajadores no deben redistribuir personalmente la información sobre la vulnerabilidad del sistema a otros usuarios.

Pruebas de Controles—Los trabajadores no deben probar o sondear los mecanismos de seguridad en la Empresa X o en otros sitios de Internet a menos que hayan obtenido un permiso por escrito del gerente corporativo de Seguridad Informática. La posesión o el uso de herramientas para detectar los aspectos vulnerables del sistema de información o para comprometer los mecanismos de seguridad de la información están prohibidos sin el permiso previo del gerente corporativo de Seguridad Informática.



Capítulo 12 MODELO DE POLÍTICA DE SEGURIDAD EN INTRANETS

Sólo para Uso del Negocio—El objetivo de la intranet en una Empresa X es facilitar al personal de dicha empresa, los procedimientos para comunicarse y conducir sus negocios con más eficiencia y efectividad. Al igual que con los otros sistemas informáticos de la Empresa X, su función está destinada al uso corporativo; por lo que el manejo de ésta con fines personales puede autorizarlo únicamente el gerente del departamento.

Respeto a los Derechos de Autor—Aunque la intranet es un medio de comunicación informal interno, las leyes y derechos de autor, las patentes y las marcas registradas permanecen vigentes. Los empleados pueden publicar su material en la intranet, siempre y cuando se sigan los siguientes pasos:

- Si el material a publicar se originó fuera de la Empresa X, es indispensable obtener un permiso de la fuente de origen y otorgar a dicha fuente el crédito correspondiente.
- Si existe la posibilidad de infringir el derecho de autor, de divulgar información confidencial, de libelos, de ataques al honor de la personas o de otros asuntos legales, el asesor legal de la Empresa X debe aprobar la publicación.
- Los trabajadores deben confirmar individualmente la veracidad, la oportunidad y la relevancia que tiene el material para la Empresa X.
- Un administrador web debe hacer una prueba operativa y de seguridad de todas las páginas web desarrolladas por usuarios, de conformidad con el proceso aprobado por el Departamento de Seguridad Informática.

Contenido Prohibido—Información secreta de la Empresa X no debe residir en los servidores de Internet o Intranet.

Control de Contenido—Los sistemas de computación y de comunicación de la Empresa X no están destinados ni deben ser utilizados para ejercitar el derecho a la libre expresión del participante. Estos sistemas, incluyendo la intranet, no deben usarse como foro abierto para discutir los cambios organizacionales, los asuntos relativos a las políticas del negocio ni otros tópicos similares de la

Empresa X. La gerencia de la Empresa X tendrá derecho a censurar, eliminar o enmendar cualquier información publicada en las redes y computadores de la Empresa X, incluyendo la intranet.

Autorización para Publicaciones—Antes de publicar cualquier información en la intranet de la Empresa X, debe obtenerse la autorización del administrador encargado de la página intranet correspondiente, así como la del Propietario de la información en cuestión o, en su defecto, la del creador de la información en caso de no haberse asignado aún un Propietario. En algunos casos, ambas autorizaciones pueden provenir de la misma persona. Debe seguirse un procedimiento formal de control de cambios para efectuar cambios al contenido publicado en la intranet de la Empresa X, y dicho procedimiento debe incluir la documentación de las autorizaciones gerenciales y el archivado de todas las versiones anteriores del material publicado. Si se han de utilizar programas de actualización automática de software y datos desde Internet a través de la intranet de la Empresa X, estos acuerdos deben seguir el mismo proceso formal de control de cambios.

Clasificación de las Publicaciones—El contenido publicado en la intranet de la Empresa X debe ser clasificado o bien como Público o bien como Sólo para Uso Interno. Nunca se debe incluir información Secreta o Confidencial en la intranet de la Empresa X. El personal del Departamento de Seguridad Informática debe revisar trimestralmente las publicaciones de la Empresa X para confirmar que ninguna contenga información Secreta o Confidencial.

Propiedad Legal del Material Publicado—A menos que sea autorizado con anticipación por el director del Departamento de Tecnología Informática, y explícitamente notificado en la página de intranet, todo contenido incluido en la intranet de la Empresa X es propiedad de la Empresa X.

Designación del Propietario de la Información—Todo contenido publicado en la intranet de la Empresa X debe tener un Propietario designado. La información de contacto de este Propietario debe estar claramente indicada en la página donde aparece el contenido.

Sistemas de Producción—Todos los servidores de intranet se consideran sistemas de producción y, por ende, deben satisfacer todos los requisitos especificados en la Metodología de Desarrollo de Sistemas para los sistemas de producción. Dichos requisitos incluyen la asignación formal de responsabilidades, el adiestramiento adecuado del personal que labora en el sistema de producción, por lo menos dos empleados adiestrados y técnicamente competentes para manejar el sistema, respaldos periódicos y actualizaciones frecuentes del software.

Acceso de Terceras Personas—Todo acceso a los sistemas internos de los computadores de la Empresa X que no estén específicamente identificados como públicos, tales como la intranet, debe estar autorizado con anticipación por el gerente de Seguridad Informática.

Diseminación Restringida—La intranet de la Empresa X es para uso exclusivo de las personas autorizadas, y la información allí contenida puede ser divulgada sólo a personas autorizadas. Los empleados no deben remitir a tercera personas ninguna información que aparezca en la intranet sin consultar con los canales internos correspondientes, tales como Mercadeo, Recursos Humanos o Relaciones Públicas.

Normas y Recursos Relevantes—Todas las páginas de intranet deberán seguir las normas de diagramación, navegación y vocabulario, así como cualquier otro requisito similar estipulado por el comité de administración de la intranet. Todo el personal que desarrolle sitios de intranet debe observar sistemáticamente la guía de estilo y utilizar los recursos que se encuentran en el repositorio de implementación de la intranet.

Conexiones con los Sistemas de Producción—La intranet no debe utilizarse para efectuar conexiones en tiempo real con ningún sistema informático de producción de la Empresa X que posea controles extendidos de acceso para la autenticación del usuario, lo cual es

cualquier procedimiento que exige más que la simple contraseña fija y el identificador del usuario, a menos que haya sido autorizado por el gerente del Departamento de Seguridad Informática.

Conexión de Sistemas a la Intranet—Antes de conectar a la intranet de la Empresa X cualquier sistema de computación, segmento de red o algún mecanismo de acceso a la red, como por ejemplo, un modem, se tiene que considerar si satisface el criterio de seguridad establecido por el gerente de Seguridad Informática. Estos criterios incluyen, sin limitantes, lo siguiente: ninguna conexión a intranet que no esté protegida por un cortafuego aceptable, un sistema aceptable de autenticación del usuario, un sistema aceptable de control de privilegios de usuarios, un proceso establecido de control de cambios, una definición claramente escrita de las responsabilidades de la gerencia y la documentación operativa correspondiente.

Autorizaciones de los Servidores—Antes de hacer cualquier conexión a la red interna, todos los servidores de intranet deben estar autorizados de antemano por el gerente de los servicios de red del departamento de Tecnología Informática. Dicho proceso de autorización consiste en garantizar que todo software autorizado, tal como el programa antivirus, se instaló adecuadamente. Este proceso corrobora que se probaron apropiadamente todos los subprogramas (applets) de contenido activo y, asimismo, garantiza que se utilizan protocolos de red y hardware compatibles con el mismo.

Establecimiento de Enlaces con Internet—No están permitidos los vínculos que transfieren la sesión del usuario desde el sitio de intranet de la Empresa X al sitio web de cualquier entidad externa, a menos que se obtenga de antemano la aprobación del gerente del departamento de Seguridad Informática. Cada vez que se establezcan, estos enlaces deben notificar claramente al usuario que está abandonando la intranet de la Empresa X y entrando en Internet.



Capítulo 13 MODELO DE POLÍTICA DE PRIVACIDAD — ESTRICTA

BOSQUEJO Y APLICABILIDAD

La Empresa X apoya el derecho a la privacidad, incluyendo los derechos de los individuos para controlar la divulgación y el uso de sus datos personales, sus preferencias o experiencias. La Empresa X apoya las leyes nacionales e internacionales y los reglamentos que exigen la protección de los derechos a la privacidad de dichos individuos.

Esta política se aplica a todos los empleados de la Empresa X, contratistas, personal temporal y consultores, además de otros trabajadores. Se espera que todas estas personas estén familiarizadas y totalmente en conformidad con estas políticas. Los trabajadores que no la cumplan estarán sujetos a acciones disciplinarias, incluyendo el despido.

Esta política también se aplica a las empresas contratistas que proporcionen servicios de procesamiento de información en beneficio de la Empresa X. Cuando se contrate una empresa para procesar datos personales, debe incluirse siempre una obligación contractual que consistentemente observe estas políticas y los procedimientos y normas relacionados con la Empresa X, tal y como los especifique el departamento de Seguridad Informática. Toda empresa contratista que maneje datos personales suministrados por la Empresa X, periódicamente debe emitir certificados de acatamiento de estas políticas y, además, permitir que la Empresa X inicie auditorias independientes para determinar el cumplimiento de estas políticas.

DEFINICIONES

Datos Personales—Cualquier información relacionada con un individuo que incluya nombre, dirección, número telefónico, número de seguridad social, número de la licencia de conducir y detalles de transacciones comerciales de índole personal. Por ejemplo, dicha persona podría ser un comprador de los productos de la Empresa X. Las siguientes políticas no se aplican a los informes estadísticos ni a otros grupos de información en los que una persona natural no sea específicamente identificable.

Procesamiento de datos personales o "procesamiento"—Cualquier operación o conjunto de operaciones que se efectúe sobre datos personales, mediante procesamiento automático, como recaudación, grabación, organización, almacenaje, adaptación o alteración, extracción, consultoría o lo contrario, por razón de disponibilidad, combinación, bloqueo, borrado o destrucción.

Propietario—El administrador o ejecutivo de la Empresa X que determina los fines del procesamiento de los datos personales y que toma las decisiones acerca del mecanismo de seguridad a utilizarse para proteger dicha información personal.

Custodio—El gerente de la Empresa X, o el de una tercera organización si el procesamiento ocurre fuera de la empresa, quien procesa los datos personales en concordancia con las instrucciones impartidas por el Propietario.

Terceros—Cualquier persona, sociedad, compañía, autoridad pública, agencia gubernamental o cualquier otra entidad distinta a un individuo, Propietario, Custodio y las personas que, por mandato directo del Propietario o Custodio, estén autorizadas para procesar los datos.

Receptor—La persona, autoridad pública, agencia gubernamental, o cualquier otra entidad a quien se revelen datos personales, aunque el destinatario sea un tercero.

Consentimiento—Cualquier indicación proporcionada libre e informadamente, donde el individuo expresa su deseo y manifiesta su conformidad de que sus datos sean procesados y, de ser necesario, revelados.

En esta política no se hace distinción alguna entre datos, información, conocimiento o sabiduría.

REQUERIMIENTOS ESPECÍFICOS

- 1 Todos los datos personales deben procesarse de manera equilibrada y legal, de acuerdo con las leyes y reglamentos de todas las jurisdicciones donde la Empresa X haga negocios.
- 2 Los datos personales deben recolectarse para los fines ya informados a la persona y no para otros efectos. El procesamiento adicional de los datos con fines históricos, estadísticos u otros fines empresariales no es incompatible, siempre y cuando dichos procesamientos adicionales incluyan mayores controles para proteger los derechos del individuo.
- 3 La cantidad de datos personales recolectada debe ser la adecuada, la correspondiente y la necesaria respecto de los fines para los cuales fue recaudada o para la necesidad del procesamiento adicional requerido.
- 4 Los datos personales deben ser precisos, completos y, en caso necesario, mantenerse actualizados. Deben seguirse todos los pasos razonables para garantizar que los datos personales incorrectos o incompletos se borren o corrijan definitivamente, siempre dentro de los fines para los que fueron recaudados, o para su procesamiento adicional.
- 5 Las personas deben recibir la oportunidad de examinar sus datos personales y de emitir quejas por errores y registros incompletos. Las investigaciones de las quejas deben ejecutarse con prontitud, contestándose por escrito e informando a la persona interesada sobre las medidas correctivas que tomará la Empresa X. Cualquier corrección o eliminación de datos debe ejecutarse con prontitud y sin costo alguno para el individuo. Asimismo, deben tomarse precauciones razonables para evitar reincidir en los mismos errores u omisiones. Ello puede lograrse agregando un párrafo explicativo en el archivo correspondiente de la persona afectada. Se permitirán excepciones a los requerimientos establecidos en este párrafo en casos de registros de planificación de sucesión gerencial, de registros de investigación de actividades ilegales y de otras actividades comerciales legítimas, donde la divulgación al individuo pondría en alto riesgo el proyecto en marcha.
- 6 Los datos personales no deben guardarse de manera que se permita la identificación de los individuos por más tiempo del necesario, de acuerdo con los fines para los que fueron recaudados o para los que deba realizarse procesamiento adicional. Por ejemplo, esto se puede implementar con archivos separados pero enlazados, donde uno contenga la información sobre su identificación y el otro la información confidencial correspondiente.

Los Propietarios de los datos personales son responsables de garantizar el cumplimiento de los elementos correspondientes a los puntos anteriores.

- 7 Los datos personales se pueden procesar únicamente si:
 - La persona ha otorgado su consentimiento sin ambigüedades.
 - El procesamiento es necesario para cumplir un contrato del cual el individuo es parte interesada, como por ejemplo un pedido de productos.
 - El procesamiento es un requisito para responder a una petición hecha por el individuo.
 - El procesamiento es necesario para lograr el cumplimiento de una obligación legal que pesa sobre el Propietario.
 - El procesamiento es necesario para proteger los intereses vitales del individuo.
 - El procesamiento es necesario para explorar o proporcionar productos o servicios comerciales innovadores que puedan ser útiles para el Propietario, siempre y cuando estos productos o servicios no menoscaben los derechos fundamentales o libertades del individuo.

8 Queda prohibido el procesamiento de datos personales que pongan al descubierto la raza u origen étnico, opiniones políticas, creencias religiosas o filosóficas, membresías en sindicatos laborales, prontuarios policiales, salud o vida sexual, a menos que:

- El individuo haya suministrado su consentimiento explícito para tal procesamiento.
- El procesamiento sea necesario para efectos del cumplimiento de las obligaciones y de la preservación de los derechos específicos del Propietario, de conformidad con la ley del trabajo.
- El procesamiento sea necesario para proteger los intereses vitales del individuo o de otra persona que no pueda dar su consentimiento por incapacidad física o legal.

Los custodios de datos personales son los responsables de garantizar el cumplimiento de los elementos de los dos puntos anteriores.

INFORMACIÓN A SUMINISTRAR A LA PERSONA

El Propietario o su representante deben suministrar a las personas la siguiente información:

- La identidad del Custodio y la de su representante, si lo hubiere.
- Los fines del procesamiento al cual se someterán los datos.
- Las políticas relacionadas con el manejo de datos personales, incluyendo las modificaciones materiales efectuadas a las políticas que hayan entrado en vigencia después de la recaudación de los datos personales.
- Cualquier información adicional, como por ejemplo:
 - Los receptores o categorías de receptores de los datos.
 - Si las respuestas son obligatorias o voluntarias y las posibles consecuencias en caso de no responder.
 - El derecho a exigir el acceso y a corregir los datos relacionados con la persona.

Cuando los datos personales no se han recibido directamente de la persona, el Propietario o su representante deben notificarlo en el momento de procesar los datos. Si se prevé la divulgación a un tercero, se debe notificar

a la persona de manera previa al momento de revelar los datos. El Propietario debe proporcionar a la persona por lo menos la siguiente información, a menos que el individuo ya la maneje:

- La identidad del Custodio y la de su representante, si lo hubiere.
- Los fines del procesamiento.
- Cualquier información adicional, como por ejemplo:
 - Las categorías de datos involucrados.
 - Los receptores o categorías de receptores.
 - El derecho a exigir el acceso y a corregir los datos relacionados con la persona.

A solicitud, el propietario o su representante deben proporcionar a la persona un resumen por escrito de su derecho de saber sobre sus datos personales, obtener copias de ellos, manifestar objeciones al respecto y corregirlos. Debe disponerse de personal calificado para explicar a las personas vía telefónica sus derechos.

Si la Empresa X cambia su política de privacidad, prontamente debe iniciarse un intento para notificarlo a los interesados. Como parte de esta notificación, la Empresa X debe proporcionar a las personas un resumen de las palabras que han cambiado y su signifi-

cado. Las personas deben recibir la oportunidad de elegir si desean eliminar sus datos de los archivos de la Empresa X

DERECHO DE LAS PERSONAS A ACCEDER A LOS DATOS

Toda persona tiene derecho a recibir del Custodio lo siguiente:

- 1** Sin restricciones injustificadas, a intervalos razonables y sin demoras ni gastos excesivos:
 - La confirmación de que los datos que les conciernen han sido procesados y como mínimo la información acerca del objetivo del procesamiento, las categorías de los datos en referencia, y los receptores o categorías de receptores a quienes se revela la información.
 - Los detalles acerca de la fuente de información de los datos sobre la persona, si la información está registrada.
 - La comunicación de los datos personales a la persona en forma inteligible.
 - El conocimiento de la lógica involucrada en cualquier procesamiento automatizado de los datos de la persona, por lo menos en el caso de las decisiones automatizadas que la afecten.
- 2** La notificación, cuando corresponda, de que sus datos personales han sido corregidos, borrados, o bloqueados debido a que estaban incompletos o errados.
- 3** La notificación a terceros a los cuales se han divulgado los datos respecto de cualquier corrección, eliminación o bloqueo llevado a cabo según lo indicado en el párrafo que antecede, a menos que esto sea imposible o implique esfuerzo y gasto excesivo.

DERECHO DE LA PERSONA A OBJETAR

Las personas tienen derecho a objetar, sin costo, por el procesamiento de los datos personales que el Propietario suponga se procesarán para efectos de mercadeo directo. Los Propietarios deben contar con mecanismos rápidos de procesamiento que permitan a individuos objetantes ser removidos de las listas de mercadeo directo.

Los individuos deben ser informados antes de que sus datos personales sean revelados por primera vez a terceros o utilizados en su nombre para efectos de mercadeo directo. También los individuos deben recibir el ofrecimiento del derecho a objetar, sin costo alguno, a dicha revelación o utilización. Los Propietarios deben proporcionar mecanismos de procesamiento que permitan a los objetantes bloquear la divulgación.

DIVULGACIÓN DE DATOS PERSONALES A TERCEROS

La Empresa X puede proporcionar a terceros la información personal procesada en sus sistemas por razones normales, tales como mandatos y citaciones de tribunales, constancias de trabajo, licencias gubernamentales, seguros y otras. Los solicitantes de tal información deben obligatoriamente identificarse, certificar por escrito las razones, legales o no, por las que requieren la información y certificar que los datos personales no se utilizarán para otros propósitos.

Toda divulgación a agencias gubernamentales o a otros terceros tiene que estar precedida por una notificación escrita enviada al individuo. Una sola autorización general será suficiente para cubrir tales divulgaciones. Se debe proporcionar el tiempo suficiente entre la recepción de la notificación y la divulgación de los datos a terceros, para que el individuo pueda objetarla, en caso de que así lo deseé.

CONFIDENCIALIDAD Y SEGURIDAD DEL PROCESAMIENTO

El Propietario debe implementar medidas técnicas y estructurales apropiadas para proteger los datos personales contra la destrucción ilícita o accidental y pérdidas fortuitas, así como alteraciones, revelaciones y accesos no autorizados. Estas medidas deben estar dentro de la normativa establecida por el departamento de Seguridad Informática.

No debe efectuarse la transferencia de información privada a otro país, sin importar la tecnología empleada, hasta tanto se tenga la aprobación por anticipado del gerente de Seguridad Informática. Se pueden hacer excepciones en aquellos casos en que la persona se encuentre, se encontraba o se encontrará en el país de destino, o en el caso de que haya solicitado específicamente dicha transferencia.

Ningún sistema informático de la Empresa X, como tampoco sus empleados, debe vincular información anónima acerca del comportamiento de una persona con la información de aquellas actividades identificadas como personales, a menos que las mismas personas en cuestión lo autoricen. Es el caso cuando tal vinculación puede enlazar información de compras por Internet con registros del explorador.

El Propietario o su representante oficial deben preparar una evaluación de riesgo documentada para determinar las implicaciones sobre la privacidad de cualquier uso nuevo o diferente, pero significativo, de los datos personales. Dicha evaluación de riesgo debe efectuarse antes de que ocurra la utilización de los datos y debe contener todos los pasos del procesamiento propuesto, incluyendo el acceso, el almacenaje, la transmisión y la destrucción de la información. La evaluación debe comprender no solo la consideración de los riesgos, sino también las medidas de seguridad a emplear tales como los controles de acceso, los cifrados, los registros, los cronogramas de retención de los datos y los procedimientos de destrucción de los mismos.

Los desarrolladores no deben usar datos verdaderos cuando construyan, prueben, mejoren y hagan mantenimiento a los sistemas de procesamiento. Por el contrario, deben usar datos personales ficticios o preparados que mantengan las características de los datos, pero sin relaciones con personas identificables. En situaciones de emergencia donde se requiera el procesamiento con datos personales verdaderos, el uso de la información se permite bajo estrictos procedimientos de seguridad definidos por Seguridad Informática.

Todo acceso a los sistemas de procesamiento y redes que contengan datos personales debe registrarse para poder rastrear los accesos recientes a los datos personales de un usuario específico. Los Custodios de estos sistemas y redes son los responsables de supervisar esos registros y hacer el seguimiento de los incidentes pertinentes a la seguridad.

Cuando no estén en uso, los datos personales deben almacenarse en forma cifrada si se mantienen en un computador o en la red, o bien en archivadores cerrados o cajas similares de seguridad si se almacenan en papel, microfichas, o cualquier otra forma no computarizada. Cuando se envíen por redes públicas como Internet, deben protegerse mediante el cifrado. La normativa emitida por la Seguridad Informática contiene detalles adicionales sobre estos temas.

Cuando ya no se necesiten, todas las copias de los datos personales y sus cintas de respaldo deben destruirse definitivamente según las normas y procedimientos establecidos por el departamento de Seguridad Informática. Debe elaborarse un documento que describa la información personal destruida y presente las razones de cada proceso de destrucción realizado, y enviarse lo antes posible al Propietario correspondiente. La destrucción de los datos personales sólo puede autorizarla el Propietario, y sólo si se han cumplido todas las normas de Seguridad, los períodos legales de retención y los requisitos empresariales. Es contrario a esta política el uso de cookies, imágenes y otras técnicas para obtener información secretamente sobre las personas que utilizan Internet. Cada vez que la Empresa X obtenga información sobre las personas, ellas mismas tienen que aprobar dicha actividad. Por la misma razón, la Empresa X no deposita cookies en los discos duros de las personas ni efectúa ningún registro disimulado de las actividades que las personas desarrollan en Internet.

La Empresa X perfecciona y agiliza todas sus interacciones empresariales computarizadas con las personas, pero a la vez es clara y directa sobre sus políticas de seguridad. Para respaldar estos objetivos y motivar a las personas a usar los sitios comerciales de Internet, además de otros sistemas comerciales computarizados, la Empresa X adopta y respalda toda la normativa aceptada para evaluar el contenido y proteger la privacidad del sitio web, así como la seguridad del comercio en Internet y los sellos aprobatorios emitidos por terceros.

La Empresa X no emplea identificadores externos que puedan tener sentido para personas ajenas a su entorno como sustitutos de sus números de cuenta individuales internos. Por ejemplo, para evitar robos de identidad, la

Empresa X nunca utiliza en números de cuenta de clientes los números correspondientes al seguro social, licencias de conducir o ninguna otra identidad que un tercero pueda utilizar en forma no autorizada.

MONITOREO DE ACTIVIDADES INTERNAS

En términos generales, la Empresa X no se ocupa de monitorear todas las comunicaciones internas. Sin embargo, sí se reserva en todo momento el derecho de monitorear, tener acceso, recuperar, leer o divulgar comunicaciones internas cuando exista una necesidad empresarial legítima que no se pueda satisfacer de otra manera, cuando la persona involucrada no esté disponible y el lapso de tiempo disponible no sea suficiente para la culminación de una actividad empresarial, cuando exista motivo fundamento para sospechar actividad ilegal o violación de política, o bien cuando haya exigencia de ley, reglamento o por acuerdo con terceros.

En cualquier momento, la Empresa X puede registrar los sitios web visitados, los archivos descargados, y el intercambio de información sobre Internet. Asimismo, la Empresa X puede revisar los números telefónicos discados a través de sus sistemas. Los gerentes departamentales pueden recibir informes detallados del uso de éstos y otros sistemas de información internos, y son responsables de determinar que el uso es razonable y que está relacionado con los negocios de la empresa.

Todos los archivos y mensajes almacenados en los sistemas de procesamiento de la Empresa X se respaldan periódicamente en cintas, diskettes y otros medios de almacenamiento. Esto significa que la información almacenada en los sistemas de procesamiento de la Empresa X frecuentemente es recuperable, aunque un trabajador la borre, pudiendo examinarla más adelante los administradores del sistema u otras personas designadas por la gerencia.

La gerencia de la Empresa X se reserva el derecho a examinar sin previo aviso y en cualquier momento el correo electrónico archivado, los directorios de los archivos en los computadores personales, los archivos en los discos duros, además de cualquier otra información que se encuentre almacenada en los sistemas de procesamiento de información de la Empresa X, inclusive de datos personales. Esta supervisión se ejecuta típicamente para garantizar el cumplimiento de las políticas internas, apoyar la realización de investigaciones internas y para ayudar en el manejo de los sistemas de procesamiento de información de la Empresa X.



Capítulo 14 MODELO DE POLÍTICA DE PRIVACIDAD — NO ESTRICTA

INTENCIÓN DE LA EMPRESA Y RESPONSABILIDAD DE LA GERENCIA

Intenciones y Objetivos—En la trayectoria de su actividad comercial, la Empresa X tiene que registrar, almacenar, procesar, comunicar y por ende tramitar información confidencial acerca de los individuos. La Empresa X asume estas actividades con seriedad, al ofrecer sistemas totalmente legales, seguros y objetivos para manejar esta información confidencial. Dentro de sus actividades, la Empresa X mantiene consistentes tanto la aceptación generalizada de la ética de la privacidad como los patrones de prácticas comerciales.

Responsabilidades de la Gerencia—La Gerencia debe esmerarse para garantizar que toda información confidencial guardada por la Empresa X sea precisa, oportuna, apropiada y completa. La Gerencia también debe esforzarse en garantizar que toda información confidencial se utilice solamente para los fines destinados, y tomar precauciones diligentes y eficaces para evitar el mal uso que de ella se haga. Asimismo, la Gerencia es responsable de establecer los controles

adequados para garantizar que la información confidencial sea divulgada solamente a quienes tienen una necesidad legítima del negocio para tales accesos. La Gerencia debe establecer y mantener suficientes controles para garantizar que toda la información de la Empresa X esté libre de riesgos significativos de alteraciones no detectadas.

Etiqueta de Clasificación de los Datos—La Gerencia y específicamente los Propietarios de la información, deben aplicar una etiqueta de clasificación de datos que indique qué información es privada. Por ejemplo, esta etiqueta debe aparecer en las pantallas de los computadores cuando se muestre la información confidencial, al igual que debe aparecer en forma de sello en las versiones impresas. La etiqueta debe seguir a la información confidencial en cualquier forma que se presente, sin importar la tecnología utilizada para manejarla, quién la maneje y dónde resida.

DIVULGACIÓN DE INFORMACIÓN PRIVADA

Divulgación de Información Acerca de Políticas y Procedimientos—Como regla general, las políticas y procedimientos de seguridad informática se revelan únicamente a trabajadores y a personas externas elegidas, como por ejemplo los auditores, quienes tienen una necesidad legítima de negocio para esta información. La excepción predominante es la política relacionada con la información confidencial de los individuos. Todo individuo tiene derecho a recibir las normativas oficiales sobre políticas y procedimientos de la Empresa X que conciernen el manejo de su información. Asimismo, la Empresa X debe revelar la existencia de sistemas que contengan información privada y la manera en que se usa la información. La Empresa X no debe poseer ningún sistema de registro de

personal cuya existencia se oculte de ellos mismos, a menos que estén supeditados a una investigación por delitos y vulneración de políticas.

Manejo de Solicitudes de Información Privada—Todas las solicitudes de información privada provenientes de personas u organizaciones fuera de la Empresa X tienen que ser enviadas al asesor legal de la Empresa X, y todas las solicitudes de información privada que difieran de los procedimientos normales, pero que se originen dentro de la Empresa X, deben ser enviadas al director del Departamento de Recursos Humanos. Estos gerentes decidirán si se concede o no la solicitud.

MANEJO CORRECTO DE LA INFORMACIÓN PRIVADA

Recolectar Sólo la Información Necesaria—En general, la Empresa X puede recolectar, procesar, almacenar, transmitir y difundir sólo la información privada que sea necesaria para el buen funcionamiento de sus negocios. Por ejemplo, la gerencia de la Empresa X no debe recolectar información pertinente a las actividades de los trabajadores fuera de horas de oficina a menos que exista la probabilidad de que estas actividades afecten el desempeño del trabajador, o que puedan perjudicar la reputación de la Empresa X.

Destrucción de la Información Privada—Cuando no sea requerida por más tiempo, la destrucción de información privada contenida en los discos de los computadores u otros medios magnéticos debe llevarse a cabo a través de un proceso de sobreescritura. El simple proceso de borrarlo no es suficiente. El proceso de destrucción debe estar en concordancia con los procedimientos emitidos por Seguridad Informática para garantizar que la información privada o confidencial sea destruida apropiadamente.

Extracción de Información Privada—La información privada y confidencial no debe extraerse de las oficinas de la Empresa X. Para el traslado de esta información fuera de las oficinas es necesario contar con la autoriza-

ción del gerente departamental, siempre y cuando el trabajador a cargo del traslado haya completado la parte correspondiente a seguridad informática en su adiestramiento de teletrabajo y aprobado el examen pertinente. La firma de un acuerdo de confidencialidad con un tercero puede ser un requisito adicional al momento de extraer la información de las oficinas de la Empresa X. La información privada no puede ser trasladada a otro país, a menos que tenga el permiso del gerente del departamento de Seguridad Informática.

Divulgación Accidental en Pantallas—Las pantallas de los computadores personales, puestos de trabajo y otros terminales utilizados para procesar datos valiosos y confidenciales, incluyendo la información privada, deben estar colocadas fuera de la vista de los transeúntes de pasillos, la recepción u otras áreas de espera.

Divulgación Accidental en Papel—Cuando el trabajador maneje información privada, y entra a las proximidades una persona no autorizada, deben tomarse medidas inmediatas para ocultar la información. Si la información está en forma física, debe cubrirse con otro material y si está en pantalla, el trabajador debe cambiar al protector de pantalla o cerrar la sesión.

INFORMACIÓN PRIVADA EN SISTEMAS DE COMPUTACIÓN Y DE COMUNICACIONES

Expectativa de Privacidad—Todos los mensajes internos enviados por los sistemas de computación y comunicación de la Empresa X son propiedad de la Empresa X. La gerencia se reserva el derecho a examinar toda información transmitida a través de dichos sistemas y la supervisión puede hacerse sin previo aviso a las partes que envíen y reciban tal información. Debido a que los sistemas de computación y comunicación de la Empresa X deben usarse solamente para asuntos empresariales, los trabajadores no deben tener expectativas de privacidad en cuanto a la información que almacenen o envíen mediante estos sistemas.

Supervisión de Información Almacenada—La gerencia de la Empresa X se reserva el derecho a examinar los correos electrónicos, directorios privados, archivos de unidades de disco duro, y cualquier otra información almacenada en los sistemas de información de la Empresa X, en cualquier momento y sin previo

aviso. Este tipo de revisiones se hacen para asegurar el cumplimiento de las políticas internas, para apoyar la ejecución de las investigaciones internas y para asistir en la administración de los sistemas informáticos de la Empresa X.

Participación Gerencial en el Monitoreo—Cuando se monitoree el identificador de un usuario en un computador o en sus comunicaciones con propósitos disciplinarios o de investigación, debe informarse prontamente al gerente respectivo. Todo monitoreo debe registrarse para una subsiguiente revisión gerencial o para posibles usos en recursos legales o disciplinarios.

Función de Revisión del Gerente de Departamento—La Empresa X registra rutinariamente los sitios web visitados, los archivos descargados e intercambios de información en Internet. Asimismo, registra los números de teléfonos discados por cada trabajador. Los gerentes de departamento usualmente reciben informes

con detalles del uso de estos sistemas de información internos, y tienen la responsabilidad de determinar si su uso es razonable y pertinente al negocio.

Modificación de la Información Residente en los Sistemas—La gerencia se reserva el derecho a eliminar, resumir o editar cualquier información incluida en sus sistemas de computación o de comunicación, por tratarse de sistemas empresariales privados que no proporcionan garantías de libre expresión.

Uso Cotidiano de Sistemas de Respaldo—Todos los archivos y mensajes almacenados en los sistemas de la Empresa X, se respaldan constantemente en cintas, discos flexibles y en otros medios de almacenamiento. Esto significa que aunque un trabajador borre deliberadamente la información almacenada en los sistemas informáticos de la Empresa X, la mayoría de las veces se podrá recuperar para ser examinada en fecha posterior por los administradores del sistema y otros designados por la gerencia.

Monitoreo de Computadores Remotos—La Empresa X rastrea con frecuencia los computadores personales conectados a su red. Tales rastreos garantizan que los computadores remotos están operando sólo con el software autorizado y la debida licencia, libres de virus y gusanos, y que han sido utilizados sólo para propósitos empresariales autorizadas.

MONITOREO DE LAS ACTIVIDADES

Sistemas de Seguridad Física—Los trabajadores están sujetos al monitoreo electrónico de sus actividades mientras permanezcan en las instalaciones de la Empresa X. Este control se utiliza para medir el desempeño del trabajador, proteger su propiedad privada, su seguridad y la propiedad de la Empresa X. En áreas donde exista cierta expectativa de privacidad, tales como los sanitarios y vestuarios, no existirá este control electrónico.

Efectos Personales y Comunicaciones Privadas—Todos los efectos personales traídos a las instalaciones de la Empresa X están sujetos a requisas en cualquier momento y sin previo aviso. Los trabajadores que deseen mantener en privado ciertos aspectos íntimos, no deben traer sus pertenencias a las instalaciones de la Empresa X. Para mantener la privacidad de sus asuntos, los trabajadores no deben comunicarlos por medio de teléfonos, sistema de correo electrónico u otro

Cifrado de Correo Electrónico—Los trabajadores deben considerar el correo electrónico como el equivalente computarizado de una tarjeta postal. De no estar cifrado el correo electrónico que se remita, los trabajadores se deben eximir de enviar números de tarjetas de crédito, contraseñas, información de investigación y desarrollo, historias médicas, código fuente de programas de computación o cualquier otra información privada o confidencial.

Enlaces entre Diferentes Tipos de Información Privada—Sin el consentimiento previo del gerente del departamento de Seguridad Informática, no se deben configurar los sistemas informáticos de la Empresa X con nuevos enlaces entre información privada y otros tipos de información de un mismo individuo.

Pruebas con Datos Desclasificados—A menos que cuente con la autorización previa del gerente del departamento de Seguridad Informática, toda prueba de software en sistemas diseñados para manejar datos privados debe llevarse a cabo exclusivamente con información de producción que ya no contenga detalles específicos que puedan ser valiosos, críticos o confidenciales.

sistema de comunicación de la Empresa X que pueda estar bajo vigilancia y que esté destinado únicamente para el uso empresarial.

Utilización de Informantes—Cada cierto tiempo, la Empresa X utiliza informantes que pueden ser colocados en diferentes puestos internos, sin aparente diferencia de cualquier otro trabajador. La gerencia no está en la obligación de participar a los trabajadores sobre la presencia ni la naturaleza del trabajo que desempeñan dichos informantes.

Solicitudes con Pretextos—La Empresa X cree que todas las actividades de negocio deben conducirse en forma clara y honesta. Sin embargo, en ciertas circunstancias autorizadas por el director de Seguridad Física, la empresa podrá utilizar investigadores que se hagan pasar por otras personas, para probar el servicio al cliente, las políticas de seguridad, o investigar supuestos delitos.

MANEJO DE LA INFORMACIÓN DEL PERSONAL

Acceso al Archivo Personal Propio—Todo trabajador debe recibir acceso a su archivo laboral si lo solicita por escrito. Los empleados deben recibir permiso tanto para examinar como hacer una copia de la información que aparece en su archivo laboral. Si alguno objeta la exactitud, vigencia o integridad de la información que aparece en su archivo laboral, cada año puede agregar una declaración suplementaria de hasta 200 palabras.

Divulgación a Terceros—No se debe revelar la información privada sobre los trabajadores de la Empresa X a terceras personas, a menos que sea requisito de ley o que el trabajador emita su consentimiento explícito. La Empresa X no debe divulgar nombres, cargos, números telefónicos, lugares ni detalles de contacto de sus trabajadores, a menos que se requiera para actividades del negocio. Se pueden hacer excepciones cuando se trate de requisito de ley o cuando la persona interesada haya dado su consentimiento previo. Los motivos de retiro del trabajador tampoco se pueden revelar a terceros. Se pueden hacer dos excepciones para ello, una bajo autorización previa de la alta gerencia de la Empresa X y otra si la divulgación es

requisito de ley. La divulgación de cualquier información privada debe registrarla el departamento de Recursos Humanos y mantener dichos registros como mínimo durante cinco años.

Resumen de Divulgación—Si lo solicitan, los trabajadores deben recibir un resumen de toda divulgación que se haya hecho a terceras personas de su información privada. Asimismo, deben recibir suficiente información como para permitirles hacer contacto con dichas personas para rectificar errores o proporcionar información aclaratoria adicional.

Información sobre Cambio de Situación—La información concerniente al cambio de situación de un trabajador es estrictamente confidencial y no debe revelarse a nadie, a excepción de aquellas personas que realmente necesiten conocerla. Estos detalles de información sobre cambio de situación incluyen razones de retiro, jubilaciones, permisos, permisos con investigación pendiente, transferencias entre departamentos, cambios de puesto y cambios de posición a consultor o contratista.

INFORMACIÓN PRIVADA DE SOLICITANTES DE EMPLEO

Recopilación de Información Innecesaria—La información privada de los solicitantes de empleo no se puede recopilar, a no ser que sea necesaria para tomar una decisión sobre el empleo o pertinente al trabajo. Esta política se refiere al estado civil, objetivos de la planificación familiar, actividades en tiempo libre, preferencias políticas, trayectoria crediticia, educación y otros datos personales.

Verificación de Antecedentes y de Crédito—Cuando se pretenda verificar el historial crediticio o los antecedentes de un prospecto, la persona debe suministrar una autorización escrita indicando la aprobación del

proceso. Los prospectos deben recibir la oportunidad de retirar su solicitud de empleo o contrato de trabajo si deciden no divulgar su información privada a la Empresa X.

Pruebas Permisibles—Los candidatos para trabajar en la Empresa X no deben ser sometidos a pruebas antidopaje, de sida, sicológicas ni otras pruebas que puedan dilucidar su estilo de vida, asociaciones políticas o preferencias religiosas. La excepción puede hacerse si esta información es necesaria para determinar la conveniencia de colocar un candidato en una posición en especial.

INFORMACIÓN PRIVADA DE CLIENTES

Permiso para Recopilar Información—La recopilación de información privada sobre prospectos, clientes y otras personas con quienes la Empresa X conduce sus negocios es cotidiana y ha de esperarse. Sin embargo, los trabajadores de la Empresa X no deben recopilar información privada sobre los prospectos o clientes sin su previo conocimiento y consentimiento.

Consentimiento para la Utilización—Antes de que un cliente haga un pedido o de alguna manera revele información privada, los representantes de la Empresa X deben informar al cliente sobre cómo se puede utilizar esta información privada, y sobre los terceros a quienes se pueda divulgar, si los hubiere.

Recopilación de Información Innecesaria—Ni los trabajadores ni los sistemas de la Empresa X deben exigir información privada a prospectos o clientes que no se requiera para obtener información, completar una transacción, o entregar productos o servicios. Ningún producto ni servicio de la Empresa X puede negarse a persona alguna si se rehúsa a proporcionar información innecesaria. Los desacuerdos referentes a la información privada necesaria los resolverá el Jefe Legal de la Empresa X.

Contactos No Solicitados— Los clientes de la Empresa X deben recibir la oportunidad de informar que no desean el contacto a través de correo directo, telemarketing ni otras promociones similares. El personal de la Empresa X debe cumplir y respetar cabalmente estas solicitudes de los clientes. Asimismo, los trabajadores de la Empresa X deben respetar diligentemente el derecho incondicional de las personas a bloquear sus datos y a ser excluidos de las listas de correo y llamadas, bloquear la venta de sus datos a terceros y exigir que sus datos se eliminen de las listas de mercadeo directo.

Información Compartida sobre Clientes—La Empresa X no revela a terceros no afiliados información específica para su uso independiente sobre las cuentas, transacciones o relaciones de sus clientes, excepto bajo ciertas circunstancias. Estas circunstancias limitan la divulgación de la información a agencias de confianza, como por ejemplo una Oficina de Crédito cuando ésta desempeña su propia diligencia respecto de la solicitud de un cliente que quiere, por ejemplo, aumentar su línea de crédito; a aquellas circunstancias cuando el cliente solicita la divulgación, o cuando la divulgación es

requisito de ley o la ley la permite, o cuando el cliente ha sido informado sobre la posibilidad de utilizar la información para efectos de mercadeo o similares y ha recibido la oportunidad de rehusarse.

Cambio de la Estructura Empresarial—Si la Empresa X quiebra, se fusiona, es adquirida o de alguna otra manera cambia el formato legal de su estructura organizacional, la Empresa X necesitará compartir parte o toda la información de sus clientes con otra entidad para poder continuar proporcionando productos y servicios. Si ocurre tal cambio con su correspondiente transferencia de información, la Empresa X debe notificar a los clientes con prontitud.

Organizaciones Contratadas—La Empresa X puede contratar externamente la operación del manejo de la información, y quizás tenga que transmitir información sobre prospectos y clientes a terceros que ejecutarán el trabajo bajo contrato. En estos casos, los terceros involucrados deben firmar un acuerdo de confidencialidad que prohíba la diseminación posterior de la información e inhiba el uso de dicha información para fines no autorizados.

Aprobado por: [incluir nombre de ejecutivo]

Fecha de Aprobación: DD/MM/AA

Fecha de Vigencia: DD/MM/AA

Número de Versión: XX

Número de Política: XX-XXXX



Capítulo 15 MODELO DE POLÍTICA DE PRIVACIDAD EN LA WEB

Objetivos—La Empresa X ha creado esta declaración de seguridad y privacidad con el objeto de documentar y comunicar su compromiso de llevar sus negocios dentro de los más altos esquemas éticos y con los controles internos apropiados.

Compendio de Información Explícita—Nuestra página Web está disponible para su revisión sin que usted tenga que suministrar dato alguno. El formulario que aparece en la web denominado "solicitud para más información" requiere que los usuarios envíen información de contacto. Estos datos se utilizan para informar a aquellos que preguntan sobre nuestros productos y servicios, para enviar y facturar pedidos, y para manejar otros asuntos empresariales. También se utiliza para comunicarnos con los clientes cuando sea necesario. De vez en cuando, la información reunida por medio de ésta página se utilizará para anunciarle productos y servicios que pensamos serán de su interés.

Compendio de Información Secreta—Nuestra página no captura información secreta referente a las actividades específicas de ningún usuario en particular. Tampoco tenemos acuerdos con ningún otro sitio de Internet para localizar o controlar las actividades del usuario en la Web. Sin embargo, nuestra página sí genera reportes que nos permiten ver su actividad en nuestra página de manera anónima o agregada. No utilizamos cookies, buscadores ni mecanismos de contenido activo para capturar o mantener información relacionada con los usuarios sin su consentimiento previo. La única información personal que capturamos es la que nos remiten específicamente a través del formulario de "solicitud para más información". No almacenamos ninguna información persistente en su computador.

Política de Precaución con Niños—La Empresa X no intenta reunir información personal sobre niños. Si un niño nos envía información y dicha información se puede identificar como proveniente de un niño, la información será eliminada. No siempre podemos determinar el tipo de información que se genera cuando el usuario es un niño. En todo caso, no mantenemos bases de datos sobre niños.

Uso de la Información—La información personal que se nos entrega permanece en nuestro poder. La única excepción es cuando se revela información al gobierno de acuerdo con las prácticas normales, como por ejemplo la recaudación de impuestos o acatando órdenes de tribunales, tales como una citación o una orden de allanamiento. No vendemos, alquilamos, comerciamos, intercambiamos, prestamos ni transferimos esa información personal a compañías afiliadas, subsidiarias, empresas asociadas, sociedades mercantiles, casa matriz, sociedades estratégicas ni a ninguna otra organización.

Enlaces a Otros Sitios—Este sitio contiene varios enlaces a otros sitios. La Empresa X no se responsabiliza por las prácticas de seguridad o privacidad de estos sitios, los productos o servicios que ofrezcan, ni por el contenido que en ellos aparezca. La Empresa X no respalda ninguno de los productos o servicios señalados en estos otros sitios.

Medidas de Seguridad—Nuestro sitio está protegido con diversas medidas de seguridad tales como procedimientos de control de cambios, contraseñas y controles de acceso físicos. Asimismo, empleamos una variedad de mecanismos que garantizan que los datos que usted suministra no se pierdan, sean usados indebidamente o modificados sin autorización. Estos controles incluyen políticas de confidencialidad de datos y frecuentes respaldos de la base de datos.

Para Ponerse en Contacto con Nosotros—En referencia a este sitio Web, existen dos opciones relacionadas con su información personal. Si usted desea ponerse en contacto con nosotros sobre nuestros productos o servicios, entonces necesita proporcionarnos su información de contacto, para que podamos cumplir con su solicitud, pero si no desea contactarnos por nuestros productos o servicios, no obtendremos ninguna información suya, y usted no necesitará hacer nada más. Si decide tomar la primera de estas opciones, después de haber obtenido la información que buscaba, puede solicitarnos en cualquier momento que retiremos su nombre e información de contacto de nuestra base de datos. Si desea retirar su información personal de nuestra base de datos, haremos lo necesario para cumplir con su solicitud a la brevedad. Gustosamente

tramitaremos las solicitudes de corrección de errores y de cambios de dirección a través de los siguientes canales:

- Envío de correo electrónico a [insertar dirección de correo electrónico]
- Envío de correo regular a [insertar dirección física]
- Llamada a [insertar número telefónico] en horas hábiles

- Envío de fax a [insertar número de fax] a cualquier hora

Si tiene alguna pregunta sobre esta publicación de seguridad y privacidad, sobre las instrucciones de este sitio o sobre sus asuntos con nuestra empresa, puede ponerse en contacto con nosotros utilizando cualquiera de los canales de comunicación arriba mencionados.



Capítulo 16 MODELO DE POLÍTICA DE CLASIFICACIÓN DE DATOS

INTRODUCCIÓN Y BOSQUEJO

Responsabilidad del Trabajador—Todo trabajador con acceso a la información o sistemas informáticos de la Empresa X juega un papel importante en la seguridad informática de la organización. Por ejemplo, cada trabajador debe responsabilizarse personalmente por custodiar la información que le ha sido confiada. Es necesario que todos los trabajadores que entren en contacto con la información interna y delicada de la Empresa X se familiaricen con la política de clasificación de datos y que utilice permanentemente las mismas pautas en sus actividades comerciales diarias dentro de la Empresa X. La información sensible es Confidencial o Secreta, y ambas se definen en este documento más adelante. Aunque esta política sirve de guía general para lograr la protección consistente de la información, se espera que los trabajadores apliquen y amplíen estos conceptos adaptándolos a las operaciones del día a día. Este documento facilita un modelo conceptual para clasificar la información de acuerdo con su sensibilidad, y además cuenta con un bosquejo de los enfoques requeridos para proteger la información, teniendo como paradigma las mismas clasificaciones de sensibilidad.

Riesgos Mayores—El sistema de clasificación de datos de la Empresa X, tal y como se define en este documento, se fundamenta en el concepto 'necesitar conocer'. Este término significa que la información no se divulga a nadie que no tenga la necesidad comercial legítima y demostrable de recibir la información. Este concepto, cuando se combina con las políticas definidas en este documento, protegerá la información de la Empresa X contra la divulgación, la modificación, la supresión y el uso no autorizados.

Enfoque Sistemático—Un solo error en la seguridad informática puede traer consecuencias significativas a largo plazo. Es esencial el uso sistemático de este

sistema de clasificación de datos si se va a proteger correctamente la información sensible. Sin el uso continuo de este sistema de clasificación de datos, la Empresa X arriesga innecesariamente la pérdida de relaciones con clientes, la confianza del público, la interrupción operacional interna, costos excesivos y desventaja competitiva. Esta política sistemáticamente protege la información sensible, en cualquiera de las formas que adopte, la tecnología que se aplique para procesarla, quién la maneje, cualquiera que sea la ubicación de la información, y cualquiera que sea la etapa del ciclo de vida en que se encuentre.

Información Aplicable—Esta política de clasificación de datos se debe aplicar a toda la información que la Empresa X posea o tenga bajo su control. Por ejemplo, la información Confidencial confiada a la Empresa X por clientes, socios, proveedores y terceros debe protegerse con esta política de clasificación de datos. Se espera de los trabajadores que protejan la información de terceros con el mismo cuidado que protegen la información de la Empresa X. Para los efectos de esta política no se hace distinción entre los términos "datos", "información", "conocimiento" y "sabiduría".

Secretos Industriales—Uno de los tipos de información confidencial se denomina Secreto Industrial. Los Secretos Industriales son un tipo de información de propiedad exclusiva que de alguna manera le da a la Empresa X una ventaja competitiva. Este documento resguarda los Secretos Industriales, a los cuales hay que designar por separado. Los Secretos Industriales deben estar identificados como tales, previa divulgación a cualquier trabajador. Toda información sobre Secretos Industriales se predetermina como Secreta. El Consultor Jurídico Jefe es la única persona autorizada para designar cualquier información de la Empresa X como Secreto Industrial.

CONTROL DE ACCESO

Necesidad de Conocer—Cada uno de los requerimientos de políticas establecidos en este documento se fundamenta en el concepto de la necesidad de conocer. Si un trabajador no tiene claro cómo aplicar los requerimientos establecidos en esta política en una situación específica, debe valerse conservadoramente del concepto de la necesidad de conocer. Eso quiere decir que la información sólo debe divulgarse a aquellos que tienen una necesidad legítima del negocio para dicha información. Este principio se refiere a la información privada de empleados, tales como historias médicas, pero también se aplica a la información de propiedad exclusiva de una compañía, tales como los planes de un nuevo producto.

Controles de Acceso a los Sistemas—El acceso a la información confidencial residente en los computadores de la Empresa X debe protegerse mediante controles de acceso para asegurar que no sea divulgada, modificada, suprimida o eliminada. Los sistemas tradicionales de control de acceso emplean identificadores de usuario y contraseñas fijas, pero hoy en día los están desplazando las tecnologías más seguras como las contraseñas

dinámicas y los sistemas biométricos. Para cualquier tecnología que se va a emplear, el acceso de cada individuo se debe controlar fundamentándose en la necesidad de conocer. La idea de la necesidad de conocer incluye no sólo revisar la información, sino otros privilegios como modificar la información o utilizar la información para llevar a cabo una transacción. Los sistemas de control de acceso de la Empresa X deben registrar los accesos del usuario y los datos confidenciales que usó, además de la hora y fecha de dicho acceso.

Decisiones para Otorgar Acceso—El acceso a la información confidencial de la Empresa X debe otorgarse únicamente después de tener la autorización por escrito del Propietario de la información. Los Custodios de la información en cuestión deben dirigir todas las solicitudes de acceso al Propietario o delegado correspondiente. Existen plantillas normales del sistema de privilegios ya definidas para todos los cargos, y los Propietarios aprueban estos privilegios de antemano. Otros privilegios de acceso para necesidades especiales se manejan a medida que surja cada solicitud.

ETIQUETAS DE CLASIFICACIÓN

Los Propietarios y la Información de Producción—Todo tipo de información de producción que una unidad organizacional de la Empresa X posea o utilice debe tener un Propietario. La información de producción se utiliza cotidianamente para llevar a cabo los objetivos comerciales. Ejemplos de ello son el resumen de nómina, itinerarios de embarques e informes gerenciales de contabilidad de costos. Los propietarios son los responsables de asignar las clasificaciones apropiadamente según la sensibilidad como se define a continuación. Legalmente los Propietarios no son los dueños de la información confiada a ellos. Son en cambio integrantes asignados al equipo gerencial de la Empresa X que actúan como administradores, y quienes supervisan las formas en que se usan y protegen ciertos tipos de información [aquí se puede incluir un enlace a la política de propiedad de datos].

SECRETO—Esta etiqueta de clasificación corresponde a la mayor parte de la información comercial confidencial de uso interno y exclusivo de la Empresa X. Su divulgación no autorizada podría impactar seriamente y desfavorablemente a la Empresa X, sus clientes, proveedores, socios, y empleados. Ejemplos de ello son los documentos de fusión o adquisición, planes estratégicos en el ámbito

corporativo, litigios, memorandos estratégicos, informes sobre investigación de nuevos productos en innovación tecnológica y los Secretos Industriales, como por ejemplo algunos programas de computación.

CONFIDENCIAL—Esta etiqueta de clasificación corresponde a la información comercial menos delicada que se destina al uso interno de la Empresa X. Su divulgación no autorizada podría impactar desfavorablemente a la Empresa X, sus clientes, proveedores, socios, o empleados. La información que algunos pueden clasificar como privada, es la que se incluye en esta clasificación. Ejemplos de ello pueden ser las evaluaciones de desempeño de los empleados, la gestión de datos de clientes, los acuerdos de alianzas estratégicas, estudios de mercado generados internamente aún sin publicar, claves de computación, números de identificación personal en tarjeta portátil y los informes de auditoría interna.

SÓLO PARA USO INTERNO—Esta etiqueta de clasificación compete a toda otra información que no se ajuste claramente a las dos clasificaciones anteriores. Aunque la divulgación no autorizada va en contra de la política, no se espera que impacte seriamente ni desfavorable-

mente a la Empresa X ni a sus empleados, proveedores, socios, así como tampoco a sus clientes. Ejemplos de ello son el directorio telefónico de la Empresa X, los números de acceso discado del computador, los materiales de entrenamiento para empleados nuevos y los manuales internos de políticas.

PÚBLICA—Esta clasificación se refiere a la información aprobada por la gerencia de la Empresa X para hacerse pública. Esta información no se define como divulgación no autorizada y puede difundirse sin daños mayores. Ejemplos de ello son los folletos sobre productos y servicios, propagandas, anuncios sobre ofertas de trabajo y comunicados de prensa.

Otras Etiquetas—Se permiten otras etiquetas en la clasificación de datos específicos para los departamentos o divisiones de la Empresa X, pero deben ser

consistentes con el sistema de clasificación de datos. Estas etiquetas adicionales pueden incluir el uso de palabras como "Privado" o "Financiero".

Los Propietarios y las Decisiones de Acceso—Los propietarios deben tomar decisiones sobre quiénes van a tener acceso a la información, y el uso que se le dará. También deben tomar las medidas necesarias para asegurar que se utilice el control apropiado en el almacenamiento, manejo, distribución y usos normales de esta información. Los lectores de estas políticas pueden determinar rápidamente quién es el Propietario correspondiente al consultar la página de la Intranet del departamento de Seguridad Informática de la Empresa X [aquí se puede incluir un enlace a dicha página].

ETIQUETADO

Etiquetado de Clasificación—Si la información es delicada, se debe etiquetar con una denominación apropiada desde el momento en que se crea hasta el momento en que se destruye o se elimina. Esta denominación debe figurar en todos los formatos donde aparezca la información, bien sea impresa en papel, grabada en discuetos o en CD-ROM. Los trabajadores no deben quitar o cambiar las etiquetas del sistema de clasificación de datos a la información a menos que se obtenga el permiso previo del Propietario.

Qué se Debe Etiquetar—Gran parte de la información de la Empresa X se cataloga como Sólo para Uso Interno. Por ello, no es necesario etiquetar esta información. La información sin etiqueta cae dentro de la clasificación predeterminada como Sólo para Uso Interno.

Etiquetas Al Parecer Incorrectas—Si el destinatario de la información interna de la Empresa X cree que la etiqueta de clasificación que acompaña la información es incorrecta, el destinatario debe protegerla procediendo sistemáticamente con la clasificación más rigurosa entre las dos etiquetas de clasificación disponibles. Antes de utilizar esta información o distribuirla a terceros, el destinatario debe validar con el Propietario si la etiqueta actualmente asignada a la información es la correcta.

Recopilación de Información—Los trabajadores al producir o actualizar la recolección de información, son los responsables de escoger una etiqueta apropiada para la clasificación de los datos para la nueva colección. Esta etiqueta debe ser consistente con las decisiones que

tome el Propietario respectivo y generalmente debe encontrarse en la clasificación más restringida de la recolección. Por ejemplo, si se está creando una base de datos nueva, y contiene información Sólo para Uso Interno y Confidencial, toda la base de datos debe clasificarse como Confidencial. Otros ejemplos de estas colecciones incluyen un informe competitivo generado internamente, informes de la trayectoria de decisiones gerenciales, y páginas intranet con control de acceso. En el momento de la recolección, cada uno de los trabajadores que esté generando una recolección de este tipo debe notificar al Propietario respectivo de dicha colección.

Medios de Almacenamiento—Si se transfiere una información grabada de un medio de almacenamiento de un computador que se clasifique como confidencialidad de grado alto a una clasificación de confidencialidad de grado bajo, el medio que tenga la clasificación confidencial más baja debe actualizarse de manera de reflejar la clasificación de grado más alto. Por ejemplo, si la información etiquetada como Secreta se transfiere a un disquete que contenga información sin etiqueta, se debe reclasificar inmediatamente la información en el disquete como Secreta. Si la información de datos con diferente nivel de clasificación se encuentra residente en un solo computador, los sistemas de control deben reflejar los requerimientos asociados paralelamente con la clasificación de datos más restringida. En general, debido al incremento de costos y complejidad operacional, no se recomienda entremezclar la información con diferentes niveles de clasificación de sensibilidad.

Etiquetas para Información Suministrada Externamente—Con excepción de la correspondencia comercial y software con derechos de autor, toda información suministrada externamente que no sea claramente del dominio público debe recibir una etiqueta del sistema de clasificación de datos de la Empresa X. El trabajador que reciba esta información es el responsable de asignarle la clasificación apropiada a nombre de la parte externa. Cuando se le asigne una etiqueta de clasificación de la Empresa X, este integrante del personal debe preservar las advertencias de derecho de autor, los reconocimientos de autor, las pautas para interpretación y la información referente a la diseminación restringida.

Etiquetado de Copias Impresas—Toda copia impresa, manuscrita o manifestación de información confidencial debe portar evidencia clara de la etiqueta confidencial en la parte superior derecha de cada página. Si está encuadrado, toda manifestación de información delicada debe tener una etiqueta apropiada de confidencialidad en la carátula anterior, en la página del título, y en la carátula posterior. La página de envío de fax que contenga información delicada también debe contener la etiqueta de clasificación apropiada. Las microfichas y los microfilmes deben igualmente contener etiquetas, si éstos contienen información delicada.

Etiquetado de Medios de Almacenamiento Computarizados—Todos los CD-ROM, discuetes, así como otros medios de almacenamiento en el computador que contengan información delicada deben ser etiquetados externamente con la clasificación de sensibilidad apropiada. A menos que afecte desfavorablemente la operación de un programa de aplicación, o archivos de computador que contengan información delicada, debe indicarse claramente la clasificación pertinente en las dos primeras líneas de datos.

INTERACCIONES CON TERCEROS

Terceros y la Necesidad de Conocer—A menos que se designe específicamente como Pública, toda la información interna de la Empresa X debe estar protegida contra la divulgación a terceras personas. Los terceros pueden tener acceso a la información interna de la Empresa X siempre y cuando demuestren necesidad de conocer, y cuando esa divulgación haya sido expresamente autorizada por el Propietario de la información de la Empresa X. Los contratistas, consultores, empleados temporales, voluntarios y otros tipos de individuos o entidades que no sean empleados de la Empresa X, se consideran por definición terceras personas, para los efectos de esta política.

Otros Medios de Presentación—Si la información es delicada, en todo momento en que se presente en pantalla o a otro usuario debe indicarse que la información está clasificada como delicada. Las teleconferencias y llamadas en conferencia donde se discuta sobre información delicada deben ser precedidas por un enunciado que indique el grado de confidencialidad de la información. Las teleconferencias y llamadas en conferencia donde se discuta información delicada debe estar precedida por una decisión que indique que todos los participantes de la discusión están autorizados a recibir la información delicada. No deben invitarse a estas reuniones personas ajena a recibir esa información delicada.

Etiquetas Adicionales de Información Pública—A menos que sea obvia la información pública, toda información de la Empresa X que lleve una etiqueta Pública debe también portar una etiqueta "Aprobado para su divulgación pública" adjuntando la fecha en la cual el Propietario declaró Pública la información.

Grabadores y Máquinas de Dictar—Para disminuir las posibilidades de divulgación no autorizada, por lo general los trabajadores no deben grabar información delicada en maquinas de dictado, grabadores, contestadores telefónicos o en dispositivos similares. Si el uso de estos dispositivos es una necesidad operacional, debe especificarse la clasificación de sensibilidad apropiada al principio y al final de cada segmento de la información delicada. En estos casos el medio de grabación debe estar marcado igualmente con la clasificación de los datos restringidos que se encuentren en dicho medio. Debemos añadir a esto que el medio de grabación debe estar protegido en concordancia con la más estricta clasificación posible y borrarla tan pronto sea posible.

Acuerdos de Confidencialidad y Divulgación con Terceras Personas—La divulgación de información delicada a consultores, contratistas, personal temporal o cualquier otro tercero, debe ir precedida por un recibo firmado por la Empresa X evidenciando el acuerdo de confidencialidad. La divulgación de información delicada de la Empresa X a terceros debe ir acompañada por un registro que indique exactamente qué tipo de información se suministra. Este registro comprobará ser importante llegado el momento de recuperar el material u obtener el certificado de destrucción del material al final del contrato.

Acuerdos de Confidencialidad y Divulgación de parte de Terceros—Los trabajadores no deben firmar acuerdos de confidencialidad suministrados por terceros sin el consentimiento previo del Consejero Legal de la Empresa X, quien ha sido nombrado para manejar los asuntos de propiedad intelectual. Estos formularios pueden abarcar términos y condiciones que pueden restringir desfavorablemente los proyectos comerciales futuros de la Empresa X.

Solicitud de Información a la Empresa X por Parte de Terceros—Si el trabajador no ha sido autorizado por el Propietario de la información para hacer divulgaciones públicas, todas las solicitudes de información sobre la Empresa X y sus negociaciones deben referirse a Relaciones Públicas. Esas solicitudes incluyen cuestionarios, encuestas y entrevistas de prensa. Esta política no se refiere a la información de ventas y mercadeo de productos y servicios correspondientes a la Empresa X, como tampoco a llamadas de servicio al cliente.

MANEJO Y ENVÍO

Copias—Sin el previo consentimiento del Propietario, no se deben sacar fotocopias o imprimir copias adicionales de información confidencial. Los trabajadores deben estar conscientes de que algunas fotocopiadoras y fax de la Empresa X llevan registros de la información copiada o enviada por fax.

Impresión Desatendida—Las impresoras no se deben dejar desatendidas si se está imprimiendo información confidencial o se imprimirá pronto. Las personas encargadas de la impresora deben estar autorizadas para examinar la información. Sólo se permite desatender la impresión de información confidencial cuando se usa control del acceso físico para evitar que personas no autorizadas entren al área donde se encuentra la impresora y puedan ver el material que se imprime.

Uso de Servicios Externos—Antes de enviar cualquier información confidencial a un tercero para fotocopiar, imprimir, preparar formatos, u otros trabajos, la tercera parte debe firmar un acuerdo de confidencialidad con la Empresa X.

Numeración de Páginas—Toda información confidencial de la Empresa X que se manifieste en papel debe indicar el número tanto de la página actual como de la última página, por ejemplo, "Página X de Y."

Medios para Almacenar Copias de Seguridad—Toda información confidencial de la cual se haga copia de seguridad en medios computarizados y se almacene

Revisión Previa—Todo discurso, presentación, papel técnico, libro o cualquier otra comunicación que se envíe al público debe ser aprobado para su publicación por el gerente inmediato del empleado pertinente. Esta política goza de efecto si el empleado representa a la Empresa X, si trata asuntos de la Empresa X, o si la comunicación se fundamenta en información obtenida durante el transcurso de las obligaciones laborales desempeñadas por la Empresa X. Si la investigación de nuevos productos, las estrategias corporativas, la información del cliente o los proyectos de mercadeo se han de divulgar, es necesario el previo consentimiento de los directores del departamento de Investigación y Desarrollo y del departamento Legal.

Notificación al Propietario—Si la información delicada se pierde, se divulga a partes no autorizadas, o se sospecha que se ha perdido o se ha divulgado a partes no autorizadas, se debe notificar al Propietario de la información y al gerente del departamento de Seguridad Informática de inmediato.

fuerza de las oficinas de la Empresa X debe ir cifrada. Si no se utiliza el sistema de cifrado con garantía de clave para este propósito, todas las claves que se utilicen para hacer copias de seguridad deben ser suministradas al departamento de Seguridad Informática poco después de su uso inicial.

Sobres—Si se va a enviar información confidencial por correo interno, correo externo, o correo expreso, ésta debe ir resguardada en dos sobres o cajas. El sobre o contenedor no debe indicar la clasificación o naturaleza de la información contenida en él en la parte externa. El sobre sellado y opaco o contenedor interno sí debe ir etiquetado con la clasificación apropiada. Los sobres que contengan información confidencial deben ir dirigidos a una persona específica y deben portar información suficiente del remitente. Toda información confidencial de la Empresa X que se envíe por este sistema de despacho requiere la firma autorizada de un tercero en el sitio de destino.

Entrega de Resultados Computarizados—Los resultados computarizados confidenciales deben entregarse personalmente al destinatario. Estos resultados no deben dejarse en un escritorio desatendido, colocarse en recipientes no vigilados o dejarlos a la vista en una oficina desocupada. Sólo se pueden facilitar a destinatarios que posean casilleros de correo por fax protegidos por contraseña, gaveteros personales cerrados u otros métodos de seguridad física.

Retirar de las Oficinas—La información confidencial de la Empresa X no debe ser retirada de las oficinas a menos que se obtenga el consentimiento del Propietario de la información. Esta política incluye computadores portátiles con discos duros, disquetes, copias impresas, y memos en papel. Se hace la excepción con las copias de seguridad autorizadas que estén fuera del local.

Cajas de Seguridad Dentro de las Oficinas—La información confidencial en copia impresa debe ser resguardada cuando no esté en uso, aun cuando esté dentro del edificio donde el acceso esté controlado. Toda información confidencial que no esté cifrada debe protegerse bajo llave en cajas fuertes, mobiliario pesado o cualquier otro contenedor que apruebe el departamento de Seguridad Informática. Toda información confidencial que se encuentre sobre escritorios después de horas de oficina, o información confidencial que esté asequible a transeúntes después de horas de oficina, puede ser confiscada y luego ser reclamada personalmente en el departamento de Seguridad Informática.

Cajas de Seguridad Fuera de Sede—Cada vez que una versión impresa de información confidencial sea retirada de las oficinas de la Empresa X y no esté en uso, ésta debe llevarse en un maletín o caja cerrada con llave. Esta información no se debe dejar desatendida dentro de un vehículo, habitación de hotel, oficina, ni ningún otro lugar, aún cuando el vehículo o la habitación estén cerrados con llave.

DESCLASIFICACIÓN Y DEGRADACIÓN

Fechas para Reclasificación—Si se conoce la fecha de vencimiento de la información Secreta o Confidencial, ésta debe señalarse en toda la información confidencial de la Empresa X. Esto ayudará a aquellas personas que poseen información a manejarla adecuadamente, aun cuando no se hayan comunicado recientemente con el Propietario de la información. Los trabajadores que poseen información confidencial nominada para desclasificación en una fecha ya vencida, pero no se sabe si fue desclasificada definitivamente o no, deben avalarla con el Propietario de la información antes de divulgar cualquier dato a terceros.

Prórroga de Clasificación—El Propietario encargado de la información puede prorrogar en cualquier momento la clasificación actual de la información antes de la fecha de desclasificación o degradación. En este sentido, el Propietario debe cambiar la fecha de desclasificación o degradación que aparece en el documento original, notificar a todos los destinatarios conocidos y Custodios, iniciar una búsqueda eficaz de destinatarios

Advertencias verbales—Si la información confidencial se comunica verbalmente en una reunión, seminario, conferencia o presentaciones similares, el orador debe participar la confidencialidad de la información. El orador debe recordar a los asistentes usar su discreción al divulgarla a otros. El equipo de ayuda visual como diapositivas o transparencias debe incluir las correspondientes etiquetas de clasificación de datos.

Teléfonos Celulares e Inalámbricos—Los trabajadores jamás deben hablar sobre la información confidencial por celulares o teléfonos inalámbricos, a menos que se haya establecido un enlace cifrado. Por igual motivo, no debe utilizarse redes de radio local para transmitir información confidencial, a menos que haya sido aprobado un proceso de cifrado correspondiente por el departamento de Seguridad Informática y se utilice consistentemente. Los enlaces de computador establecidos con teléfonos celulares u otro sistema de difusión por ondas aéreas no deben incluir transferencia de información confidencial a menos que se sepa que el enlace está cifrado. No se debe usar el sistema de teléfono por Internet para comunicar información sensible de la Empresa X, a menos que el enlace esté cifrado. [Aquí puede insertarse un enlace con la política sobre el uso aceptable de Internet].

adicionales y notificar a los Custodios de los archivos pertenecientes a la Empresa X. Los Propietarios no deben especificar una fecha para desclasificar o degradar a menos que estén relativamente seguros de que no habrá cambios en la fecha.

Notificaciones—El Propietario encargado de la información puede desclasificar o degradar la información que le ha sido confiada en cualquier momento. Para ello, el Propietario debe cambiar la etiqueta de clasificación que aparece en el documento original, notificar a todos los destinatarios conocidos y Custodios, y notificar a los Custodios de los Archivos de la Empresa X.

Cronograma de Revisión—Para determinar si la información se puede o no desclasificar o degradar, por lo menos una vez al año, los Propietarios deben revisar la confidencialidad asignada a la información que les ha sido confiada. Desde el punto de vista de la confidencialidad, la información debe desclasificarse o

degradarse tan pronto se considere práctico. Los Propietarios deben seguir las pautas para desclasificar o degradar tal y como se especifica en la política de propiedad de información. [Aquí se puede incorporar un enlace con dicha política].

DESTRUCCIÓN Y DISPOSICIÓN

Destrucción y Disposición—Toda información de la Empresa X debe destruirse o descartarse de alguna manera cuando ya no sea necesaria para efectos del negocio. Para respaldar esta política, los Propietarios de la información deben revisar el valor y la utilidad de la información periódicamente. Los Propietarios también deben revisar el cronograma de retención de documentos emitido por el departamento Legal para determinar los períodos mínimos de retención [aquí se puede insertar un enlace intranet a los datos del cronograma de retención].

Destrucción y Cajas Selladas—Toda información confidencial que no vaya a usarse o no se vaya a necesitar debe ser colocada en cajas de metal destinadas para ello y cerradas con llave hasta tanto el personal autorizado por la Empresa X o una compañía confiable de servicio de destrucción la recoja. Si no hay cajas para sellar en la localidad, la información impresa en papel debe pasarse por la máquina trituradora de papel o incinerarla, mientras que cualquier otra información confidencial contenida en otros medios debe despacharse al departamento de Seguridad Física para asegurar su destrucción. Las máquinas trituradoras de papel a usar deben transformar el papel en confeti u otra forma similar, ya que las máquinas que convierten el papel en tiras no son adecuadas para este propósito. Borrar o reformatear los medios magnéticos tal como disquetes no es aceptable como método de destrucción. El departamento de Seguridad Informática aprueba el uso de programas de sobreescritura como método para destruir información confidencial en medios magnéticos, tales como los disquetes. Sólo después de usar estos programas, pueden reutilizarse, descartarse, reciclar o donarse estos medios de almacenaje que contenían información confidencial.

Autorización para la Destrucción—Los trabajadores no deben destruir o descartar información ni archivos potencialmente importantes para la Empresa X sin la autorización previa de la gerencia. La destrucción o desecho desautorizado de la información o archivos de la Empresa X supeditará al trabajador a acciones disciplinarias, incluyendo acusaciones y despido. Los archivos y la información deben retenerse en caso de

No se Permite la Degradación Sin Autorización—Los trabajadores no deben mover la información ya clasificada en cierto nivel de confidencialidad a un nivel menor, a menos que este paso sea parte oficial del proceso autorizado por el Propietario para desclasificar o degradar dicha información.

necesitarse en el futuro, por motivos de regulación o estatutos que exijan su retención, o que puedan requerirse por motivos de investigación, acusación, actos improcedentes, ilegales o no autorizados. Las preguntas sobre destrucción de datos deben ser referidas al Propietario de la Información o su delegado.

Permiso para Destruir—Los trabajadores pueden destruir archivos de la Empresa X cuando el Propietario o su delegado otorgue la autorización verbal, cuando sea concedido por el Departamento de Seguridad Informática o mediante un memorando del departamento de Archivos especificando el tipo de archivos que se destruirán, la fecha o el cronograma de retención emitido por el departamento Legal. La destrucción se define como la acción que evita la recuperación de la información del medio donde se ha grabado para su almacenamiento.

Productos Intermedios—Todo material que se utilice para manejar información confidencial que podría analizarse para obtener información confidencial, debe destruirse de acuerdo con las normas establecidas para este fin. Esta política se refiere a las cintas de máquinas de escribir, hojas de papel carbón, plantillas de esténciles mimeográficos, negativos de fotografías, salidas de impresión abortadas y fotocopias inaceptables.

Fotocopias—Todas las copias desecharables de Información Secreta que se hayan generado en el transcurso de fotocopiado, impresión u otro manejo de información confidencial, deben destruirse en concordancia con las instrucciones que se encuentran en esta política. Si se traba la fotocopiadora o deja de funcionar mientras el trabajador está haciendo las copias de la información Secreta, el trabajador no debe separarse de la máquina hasta tanto todas las copias de la información sean removidas de la máquina o destruidas sin que queden rastros de ella.

Descarte de Equipos o Envío a Servicio—Toda información confidencial debe descartarse o destruirse de acuerdo con los métodos aprobados por el departamento de Seguridad Informática, antes de enviar un

computador o equipo de comunicación a un vendedor para negociarlo, darle servicio, o deshacerse de él. Los discos duros internos y otros medios de almacenaje no pueden ser donados, desecharlos en la basura, como

tampoco reciclados, a menos que hayan sido sometidos a un proceso de sobreescritura aprobado por el departamento de Seguridad Informática.

SEGURIDAD FÍSICA

Acceso a la Oficinas—Toda oficina, sala de computación y área de trabajo que contenga información confidencial debe tener el acceso físico restringido. La gerencia responsable del personal que trabaja en estas áreas debe consultar al departamento de Seguridad Física para determinar el método de control de acceso más adecuado.

Mantener Bajo Llave Cuando No Está en Uso—La información confidencial debe estar protegida de divulgación no autorizada siempre que no esté en uso. Cuando se deje desatendida, la información debe guardarse en cajas cerradas con llave. Si el Custodio de esta información sabe que va a estar ausente por menos de 30 minutos, puede dejar la información en el

escritorio o algún otro lugar a la vista, siempre y cuando todas las ventanas y puertas de la sala de donde se ausente estén cerradas con llave.

Observación No Autorizada de Pantallas—Las pantallas de computadores que manejan información confidencial deben posicionarse de manera tal que personas ajena no puedan ver la información por encima del hombro de la persona que utiliza la oficina. Igualmente, las pantallas se deben posicionar de manera tal que no sean visibles desde ventanas o ventanales por una persona que utilice binoculares o telescopios.

CONSIDERACIONES ESPECIALES EN INFORMACIÓN SECRETA

Verificación de Antecedentes—Los trabajadores que vayan a recibir acceso a información Secreta deben pasar por una verificación de antecedentes realizada por el departamento de Recursos Humanos. El acceso a la información Secreta no debe concederse mientras no se cumpla este requisito.

Almacenamiento en el Computador Personal—Si la información Secreta se va a almacenar en un computador personal, un computador portátil, asistente digital personal, o cualquier otro sistema de usuario único, el sistema debe mantener y continuamente ejecutar un paquete de control de acceso aprobado por el departamento de Seguridad Informática. Cuando el usuario no esté utilizando la información Secreta en el momento o trabajando en ella, el usuario no debe dejar desatendido el computador sin cerrar sesión o invocar un protector de pantalla o sin restringir de alguna manera el acceso a la información Secreta.

Numerar Copias de Documentos—Todas las copias de documentos Secretos deben numerarse individualmente en secuencia para asegurar que sean fácilmente localizables tanto la persona responsable por los documentos como su ubicación. Las copias impresas de

información Secreta deben exhibir la siguiente leyenda "No Copiar sin Permiso Explícito del Propietario de la Información".

Registro de Información Secreta—Cuando se trate de información Secreta, el Propietario o delegado del Propietario debe mantener un registro que refleje el número de copias obtenidas, la ubicación de las copias, los nombres de los destinatarios, la dirección de los destinatarios, así como las otras personas que tengan acceso a las copias. Este registro debe mantenerse por el tiempo que se retenga la información con la clasificación Secreta. Este registro también debe clasificarse como Secreto. Todo sistema de aplicación de producción que maneje información Secreta de la Empresa X, debe generar registros que demuestren todas las inclusiones, modificaciones y eliminación de dicha información Secreta.

Retiro de las Oficinas—La información Secreta de la Empresa X no debe salir de las oficinas de la Empresa X, a menos que cuente con la aprobación del gerente de Seguridad Informática.

Correo Expresso—El envío de la información Secreta en forma impresa debe ser encomendado a un correo expreso de confianza o enviado por correo certificado. Otra vía como el correo normal está prohibida. El envío

de la información Secreta debe manejarse en forma tal que el propio destinatario sea quien notifique el recibo de la información. Los envíos de información Secreta a intermediarios, como por ejemplo las recepcionistas, están prohibidos.

Traslado con Computadores—Los trabajadores que posean computadores portátiles, tales como laptop, notebook, asistente digital personal u otro tipo de computador que contenga información Secreta de la Empresa X, no deben dejar los computadores desatendidos en ningún momento, a menos que la información Secreta haya sido cifrada. Si se deben trasladar los datos Secretos a medios de almacenamiento legibles por computadores, deben hacerlo en forma cifrada.

Lectura en Público—Los trabajadores deben evitar los viajes en transporte público cuando posean información Secreta. Dicha información Secreta no debe leerse, discutirse y por ninguna circunstancia exponerse en aviones, restaurantes, elevadores, baños u otro lugar público. Los trabajadores de la Empresa X no deben llevar información Secreta a otros países a menos que se obtenga el permiso del gerente de Seguridad Física.

Almacenamiento—La información Secreta computarizada debe estar cifrada cuando no esté en uso. Todos los sistemas que se usen para procesar la información Secreta deben apagarse inmediatamente después de completar el proceso, o sobreescibir estos sitios de almacenamiento temporal con programas aprobados por el departamento de Seguridad Informática.

Transmisión por Redes—Si la Empresa X transmite datos Secretos por cualquier red de comunicación, debe ser sólo en forma cifrada. Estas redes incluyen el sistema de correo electrónico interno, la Internet y las líneas de discado. Tales transmisiones deben usar una red pública virtual o un software similar aprobado por el departamento de Seguridad Informática.

Transmisión a Otro Computador—Antes de transferir cualquier información de un computador a otro, la persona que se dispone a hacer la transferencia debe

asegurarse de que los controles de acceso en el computador de destino sean del mismo orden de los que provienen del computador original. Si no se puede comprobar la seguridad de los controles de acceso del sistema de destino, la información no debe ser transferida.

Transmisión por Fax—La información Secreta no debe ser enviada a un teléfono de fax que no esté atendido, a menos que la máquina de destino esté en una sala bajo llave de la cual tenga llave sólo el personal autorizado para recibir la información. La transmisión a un servidor de fax que utiliza contraseñas para el control de acceso de los faxes recibidos es una excepción autorizada de esta política. Todas las transmisiones de fax que contengan datos Secretos también deben emplear un enlace cifrado.

Teléfonos con Parlantes—La información Secreta no debe discutirse por teléfonos con parlantes, a menos que los participantes confirmen que no hay personas no autorizadas en las proximidades que puedan oír la conversación. Los trabajadores deben abstenerse de dejar mensajes que contengan información Secreta en contestadores de teléfonos o sistemas de mensajes de voz.

Conversaciones Telefónicas—Los trabajadores deben tomar medidas para evitar conversaciones sobre información confidencial por teléfono. Si la conversación sobre la información es indispensable, los trabajadores deben utilizar terminología clave y abstenerse de mencionar detalles delicados innecesarios para concluir su trabajo.

Aprobado por: [incluir el nombre del ejecutivo]

Fecha de Aprobación: DD/MM/AA

Fecha de Vigencia: DD/MM/AA

Número de Versión: XX

Departamento Responsable: [insertar nombre de departamento responsable]



Capítulo 17 MODELO DE TABLA DE REFERENCIA RÁPIDA DE CLASIFICACIÓN DE DATOS

Tabla 17-1: Tabla de Clasificación ALTAMENTE RESTRINGIDA

Acciones	Requisitos
Almacenamiento en Medios Fijos	Cifrado
Almacenamiento en Medios Intercambiables	Cifrado
Copiado	Permiso del Propietario Obligatorio
Envío de Faxes	Vínculo Cifrado y Buzón de Correos del Receptor Protegido por Contraseñas
Envío por Red Pública	Cifrado
Eliminación	Trituración o Cajas Seguras para Eliminación
Divulgación a Terceros	Autorización del Propietario y Acuerdo de Confidencialidad
Etiquetado Electrónico Obligatorio	Etiquetas Externas e Internas
Etiquetado de las Copias Impresas Obligatorio	Cada Página si son Hojas Sueltas
	Portada y Reverso y Título de la Página si está encuadrado
Empacado de Correo Interno y Externo	Dirigido a una Persona Específica pero Etiquetado sólo en el Sobre Interno
Otorgamiento de Derecho de Acceso	Sólo Propietarios
Seguimiento del Proceso Mediante Registros	Receptores, Copias Elaboradas, Lugares, Direcciones, Aquellos que Visualizaron y Destrucción

Tabla 17-2: Matriz de Clasificación CONFIDENCIAL

Acción	Requisito
Almacenamiento en Medios Fijos	Cifrado o Control de Acceso Físico

Tabla 17-2: Matriz de Clasificación CONFIDENCIAL (Continued)

Acción	Requisito
Almacenamiento en Medios Intercambiables	Cifrado
Copiado	Se Recomienda la Autorización del Propietario
Envío de Faxes	Buzón de Correos Protegido por Contraseñas o Recepción Personal
Envío por Red Pública	Cifrado
Eliminación	Trituración o Cajas Seguras para Eliminación
Divulgación a Terceros	Autorización del Propietario y Acuerdo de Confidencialidad
Etiquetado Electrónico Obligatorio	Etiquetas Externas e Internas
Etiquetado en Copias Impresas Obligatorio	Cada Página si son Hojas Sueltas
	Portada y Reverso y Titulo de la Página si está Encuadrado
Empaqueado de Correo Interno y Externo	Dirigido a una Persona Específica pero Etiquetado sólo en el Sobre Interno
Otorgamiento de Derechos de Acceso	Sólo Propietarios
Seguimiento del Proceso Mediante Registros	No Obligatorio

Tabla 17-3: Matriz de Clasificación SOLO USO INTERNO

Acciones	Requisitos
Almacenamiento en Medios Fijos	Cifrado Opcional

Tabla 17-3: Matriz de Clasificación SOLO USO INTERNO (Continued)

Acciones	Requisitos
Almacenamiento en Medios Intercambiables	Cifrado Opcional
Copiado	No Existen Restricciones
Envío de Faxes	No Existen Restricciones
Envío por Red Pública	Cifrado Opcional
Eliminación	Papelera Común
Divulgación a Terceros	Acuerdo de Confidencialidad
Etiquetado Electrónico Obligatorio	Etiquetado no Obligatorio
Etiquetado de Copias Impresas Obligatorio	Etiquetado no Obligatorio
Empaqueado de Correo Interno y Externo	Sólo un Sobre sin Marcas
Otorgamiento de Derechos de Acceso	Gerente Local
Seguimiento del Proceso Mediante Registro	No se Recomienda

Tabla 17-4: Matriz de Clasificación PÚBLICA

Acciones	Requisitos
Almacenamiento en Medios Fijos	No se Recomienda Cifrado
Almacenamiento en Medios Intercambiables	No se Recomienda Cifrado
Copiado	No Existen Restricciones
Envío de Faxes	No Existen Restricciones
Envío por Red Pública	No se Recomienda Cifrado
Eliminación	Papelera Común
Divulgación a Terceros	No Existen Restricciones
Etiquetado Electrónico Obligatorio	Fecha de Publicación más Clasificación
Etiquetado de Copias Impresas Obligatorio	Fecha de Publicación más Clasificación
Empaqueado de Correo Interno y Externo	Sólo un Sobre sin Marcas
Otorgamiento de Derechos de Acceso	No Existen Restricciones
Seguimiento del Proceso Mediante Registro	No se Recomienda



Capítulo 18 MODELO DE POLÍTICA PARA LA DIVULGACIÓN DE INFORMACIÓN A TERCEROS

DETERMINAR SI LA DIVULGACIÓN ES APROPIADA

Obligación de Debido Cuidado—Dentro de lo necesario para poder llevar a cabo sus labores, los empleados de la Empresa X recibirán el acceso a la información confidencial interna. La protección adecuada de esta información es esencial si se quieren preservar los intereses no sólo de la Empresa X, sino también de los clientes y de los socios comerciales. Estos intereses incluyen el conservar sus ventajas competitivas, la protección de sus secretos industriales y la protección de la privacidad personal. Tal como se indicó en el acuerdo de confidencialidad firmado por todos los trabajadores, se debe prestar atención especial para evitar la divulgación de información confidencial interna a terceros no autorizados.

Fuentes de Información Adicional—Si bien esta política describe las consideraciones que los trabajadores deben tener en cuenta antes, durante y después de la divulgación a terceros, dichas consideraciones no pueden abarcar cada situación que se pueda presentar. Las preguntas acerca de la divulgación de información específica se deben dirigir al propietario correspondiente de la información [insertar un vínculo a los diccionarios de datos corporativos, los cuales especifican a los propietarios de los diversos tipos de información]. Adicionalmente, se espera que los trabajadores extiendan estas políticas para que concuerden con las circunstancias específicas que enfrenten, que utilicen su juicio profesional y busquen la orientación del departamento de Seguridad Informática en aquellas circunstancias donde no esté claro el manejo apropiado de la información confidencial.

Dos Tipos de Información—Para los efectos de esta política, existen esencialmente dos tipos de información. El primero de ellos ha sido autorizado para que se publique a grupos específicos, tales como clientes, agencias reguladoras o contratistas. La información catalogada como Pública, también entra en esta primera categoría. Si el ente que solicita información está dentro del grupo de receptores autorizados, o si se le ha otorgado la etiqueta Público, no hay necesidad de aprobación por parte del propietario. El segundo tipo de información no ha sido autorizado aún para divulgarse a ningún grupo,

organización o persona específica. Esta política evalúa los requisitos específicos para trabajar con la segunda categoría. Se puede obtener orientación adicional en la Política de Clasificación de la Información [inserte un vínculo Intranet para acceder a la misma].

Terceros y la Necesidad de Conocer—A menos que se haya catalogado como Pública, toda información interna de la Empresa X debe estar protegida para evitar que se divulgue a terceros en forma no autorizada. Se puede otorgar a terceros acceso a la información interna de la Empresa X, sólo si demuestran la necesidad correspondiente y si la divulgación ha sido expresamente autorizada por el Propietario pertinente de la información de la Empresa X.

Acuerdos de Confidencialidad—La divulgación de información confidencial a los consultores, contratistas, personal temporal, voluntarios, personal externo de una organización y demás terceros, debe estar precedida por una firma de un acuerdo de confidencialidad (NDC, por sus siglas en inglés). Cuando el acuerdo es con una organización, para que sea válido debe llevar la firma de un funcionario de la organización receptora. Los trabajadores no deben firmar NDC suministrados por terceros sin la autorización previa del asesor legal de la Empresa X, designado para manejar los asuntos de propiedad intelectual.

Divulgación de Información Propiedad de Terceros—Los trabajadores de la Empresa X no deben divulgar información proveniente de terceros a otros terceros, a menos que haya sido autorizado por los terceros originadores de la información o por el Propietario legal de la misma. Aún cuando se haya autorizado la divulgación de antemano, la parte receptora debe firmar un acuerdo de confidencialidad.

Solicitud de Información de la Empresa X por Parte de Terceros—A menos que el propietario de la información haya autorizado a un trabajador para que revele la información, todas las solicitudes para obtener información sobre la Empresa X y sus negocios se deben canalizar a través del departamento de Relaciones Públicas [insertar un vínculo a esa página del departa-

mento]. Tales solicitudes incluyen cuestionarios, encuestas y entrevistas. Esta política no se aplica a la información de ventas o mercadeo de los productos y servicios de la Empresa X, ni tampoco a las solicitudes de clientes sobre información cuya emisión ya haya sido autorizada.

Revisión Previa—Toda conferencia, presentación, escrito técnico, libro, u otra información a ser divulgada al público debe tener la autorización del gerente inmediato del empleado. Esta política se aplica si el empleado va a representar a la Empresa X o a discutir los asuntos relacionados con la misma, o si la comunicación se basa en información obtenida en el curso de la ejecución de las actividades de la Empresa X. Si se van a divulgar productos nuevos, resultados de investigaciones, estrategias corporativas, información del cliente o propuestas de mercadeo, se necesita la autorización del director del departamento de Investigación y Desarrollo y la del director del departamento Legal.

Divulgación de Información Relacionada con Eventos Internos—La información específica sobre los eventos internos de la Empresa X, inclusive los productos nuevos y los servicios, promoción del

personal, reorganizaciones y problemas del sistema de información, no debe ser divulgada a terceros, inclusive los medios de comunicación, sin la autorización debida del departamento de Relaciones Públicas.

Discusiones en Foros Públicos—Se debe tener cuidado al estructurar comentarios y preguntas en los boletines electrónicos, listas de correo electrónico, grupos de noticias en línea y foros correspondientes en redes públicas como Internet. También se debe estar atento a la manera de construir las frases de solicitudes de propuestas y los anuncios publicitarios solicitando ayuda, a fin de que las direcciones estratégicas, los productos nuevos y demás información confidencial no sean divulgados indirectamente. Si un trabajador forma parte de un equipo de trabajo que está desarrollando un producto o servicio no publicitado, un trabajo de investigación y desarrollo, u otros asuntos confidenciales pertinentes a la Empresa X, todos los envíos correspondientes deben pasar por su gerente antes de ser publicados en cualquier red pública. Los trabajadores deben tener cuidado de no revelar detalles acerca de los sistemas internos de la Empresa X a través de anuncios públicos.

RESOLUCIÓN DE PROBLEMAS EN LOS PROCESOS DE DIVULGACIÓN

Propietario No Asignado—Si la información interna de la Empresa X que pueda divulgarse a un tercero, no tiene un propietario designado, la decisión de divulgar esta información debe estar bajo la responsabilidad del gerente de Seguridad Informática de la Empresa X. Antes de referir tal decisión al gerente de Seguridad Informática, aquellos trabajadores que manejen una solicitud de divulgación deben consultar el diccionario de datos corporativos para determinar si ha sido asignado un Propietario [insertar vínculo al diccionario corporativo de datos, el cual informa sobre quiénes son los Propietarios de ciertos tipos de información]. Los trabajadores también pueden pedir al Custodio de la información designado que identifique al Propietario.

Información No Clasificada—Si la información que se puede divulgar a terceros no cuenta con una clasificación de información adecuada, los trabajadores deben suponer que la información es Sólo para Uso Interno de la Empresa X, y su publicación no está autorizada. La información marcada como Pública, no requiere de la autorización del propietario antes de ser divulgada a terceros.

Conservación de las Marcas—El trabajador que divulgue la información interna de la Empresa X a terceros debe conservar las marcas exteriores que indican el autor, la fecha, el número de la versión, las restricciones de uso y otros detalles que pueden ser de utilidad para determinar el uso autorizado, la vigencia, la exactitud y la pertinencia de la información. Se puede establecer una excepción, con la autorización del Propietario, en aquellos casos en donde los distintivos revelen información de la Empresa X que no puede ser divulgada a terceros.

Excepción de Responsabilidad—Es responsabilidad del propietario de la información garantizar que, cuando se revele información controversial que cambia con frecuencia, de alta incertidumbre o potencialmente dañina, a terceros, dicha información incluya la excepción de responsabilidad correspondiente. Dichos enunciados de excepción de responsabilidad, suministrados generalmente por el departamento legal de la Empresa X, incluyen palabras que limitan la responsabilidad de la Empresa X, definen los posibles usos de la información e informan a los receptores de problemas potenciales relativos a la información.

Nombres—La terminología utilizada para hacer referencia a la información emitida a terceros debe ser consistente con la terminología empleada en el diccionario de datos corporativos de la Empresa X. Se aceptan excepciones en aquellos casos en los que ciertos términos técnicos especializados no sean de fácil

comprensión para el tercero o donde el uso de tales términos revele información que la Empresa X no desea divulgar. Si existen diferencias entre la terminología utilizada en la Empresa X y la utilizada en la información divulgada a terceros, dichas diferencias deben estar autorizadas por el Propietario designado.

REGISTRO OBLIGATORIO DE LA DIVULGACIÓN

Registros de las Divulgaciones—El trabajador que revele información a terceros debe conservar registros que reflejen la información interna confidencial de la Empresa X que se ha distribuido a terceros. Tales registros deben mostrar el tipo de información divulgada, el nombre e información de contacto de los terceros que están recibiendo la información, así como la fecha de divulgación. Aunque se haya firmado un acuerdo de confidencialidad, y aunque la gerencia haya autorizado el acceso de terceros a cierta información, es responsabilidad del trabajador que divulga la información mantener registros sobre la información divulgada.

Recuperación o Destrucción—Todas las copias de información Secreta suministradas a terceros deben ser devueltas al trabajador de la Empresa X que las suministró. Dichas copias deben ser destruidas y se debe enviar un certificado de destrucción al trabajador de la Empresa X que la suministró. Tal recuperación o destrucción se debe llevar a cabo dentro del mes

siguiente al momento cuando la información deja de ser útil para todos los efectos. El trabajador de la Empresa X que suministró la información es el responsable de recuperar la información o de obtener el certificado de destrucción. El trabajador de la compañía X debe anotar la recuperación o destrucción de la información en los registros que reflejan la información divulgada.

Informe Sobre Divulgaciones Inadecuadas—Si se ha divulgado o se piensa que se ha divulgado información confidencial en forma no apropiada, dichas circunstancias se deben informar inmediatamente al Propietario correspondiente de la información. Si la información no tiene Propietario designado, se debe informar al departamento Legal inmediatamente. Es responsabilidad del Propietario si la revelación o la supuesta revelación de la información debe ser notificada a terceros, tales como reguladores bancarios gubernamentales, personal del sistema judicial, clientes y otros. Si no se ha designado ningún Propietario, esta decisión es responsabilidad del departamento legal.

PREPARACIÓN DE LA INFORMACIÓN PARA SU DIVULGACIÓN

Uso de la Mejor Información—La divulgación autorizada de la información interna de la Empresa X debe llevarse a cabo con la información más actualizada, exacta, oportuna y pertinente. El trabajador que revela la información debe estar al tanto y extraer la información del sistema de archivos, o de la copia original definitiva de dicha información dentro de la Empresa X. Si el trabajador no está al tanto del sistema de archivos, el diccionario de datos corporativo puede suministrar esta información [se podría insertar aquí un vínculo Intranet al diccionario de datos].

Actualización de Información Previamente Divulgada—Los Propietarios deben poseer una versión correcta de la información hecha pública o divulgada a terceros, si eventos posteriores la han convertido en información materialmente incorrecta o que pueda inducir a la malinterpretación. La corrección oportuna de dicha información, es especialmente importante en

aquellas circunstancias donde el público o los terceros se apoyen en dicha información para su toma de decisiones. Este requisito no se aplica si la información fue divulgada hace un año o más en el pasado, y sea poco probable que esté en uso.

Designación de Fuentes para Divulgación al Público—La información generada por la Empresa X y dada a conocer al público, debe contar con el nombre del integrante del personal designado que actuará como la fuente oficial designada y punto de contacto. Todas las actualizaciones y las correcciones hechas a información que se liberan al público deben fluir a través de dicha fuente oficial.

Divulgación por Etapas de Información Controversial—A menos que un Tribunal lo impida, la información confidencial y controversial de la Empresa X debe revelarse al público por etapas.



Capítulo 19 MODELO DE POLÍTICA DE PROPIEDAD DE LA INFORMACIÓN

Nueva Centralidad de la Información—La información ya no es algo que apoya el suministro de un producto o de un servicio. La información ahora se ha convertido en producto que ofrece la Empresa X. La información se ha convertido en una parte crítica e integral de otros productos y servicios que suministra la Empresa X. La nueva importancia de la información presenta la necesidad de que se establezcan nuevos roles y responsabilidades para protegerla y administrarla adecuadamente. Con este fin, esta política define los roles de seguridad y responsabilidad de los Propietarios, los Custodios y los Usuarios. La seguridad informática no puede seguir siendo la preocupación exclusiva de los especialistas técnicos. Un equipo mayor de especialistas debe atenderla, y dicho equipo está conformado por todo trabajador de la Empresa X que entre en contacto con información de la Empresa X o de sus sistemas informáticos.

Alcance y Aplicabilidad de la Política—Esta política se aplica al manejo de la información de producción de la Empresa X, sin tomar en cuenta el origen de dicha información. La información de producción es la información que se utiliza normalmente para llevar a cabo importantes actividades de negocio o para respaldar la toma de decisiones de la gerencia. Esta política se aplica sin importar la tecnología de manejo de información utilizada, en dónde resida la información, cómo se utiliza la información para satisfacer las necesidades del negocio y cuáles usuarios tienen acceso a la información. Esta política se aplica sin importar la ubicación geográfica, a todas las unidades de la Empresa X, a todas las sucursales y a las demás empresas controladas por la Empresa X, y a todos los terceros que lleven a cabo negocios a nombre de la Empresa X o de otras entidades.

Roles y Responsabilidades de los Propietarios—Los Propietarios de la información son gerentes ejecutivos de las unidades de negocio, con autoridad para adquirir, generar y mantener información y sistemas informáticos dentro del área de control asignada. Los Propietarios son responsables de categorizar la información para la cual han sido designados Propietarios, utilizando la clasificación definida en la Política de Clasificación de Datos [un vínculo a dicho documento por la Intranet puede insertarse aquí]. Para ayudar en los planes de contin-

gencia, los Propietarios son también responsables de categorizar la información, o los sistemas de aplicaciones específicos, de acuerdo con una escala de criticidad definida por el departamento de Seguridad Informática [se puede insertar aquí un vínculo con una página de Intranet sobre planes de contingencia]. Los Propietarios son responsables de autorizar el acceso a la información basada en la necesidad de conocer [puede insertarse aquí un vínculo a una política específica sobre seguridad informática]. Los Propietarios designados de la información son los responsables del establecimiento y la actualización de políticas escritas específicas, relacionadas con las categorías de personas a quienes se otorgará permiso para acceder a la información. A medida que sea necesario, estas políticas deben especificar limitaciones en el uso de esta información a aquéllos a quienes ha sido otorgado el acceso. El departamento de Seguridad Informática adiestrará y suministrará material de referencia y asesoría a los Propietarios, con el fin de que puedan establecer distinciones y tomar decisiones en la forma adecuada. Los Propietarios también deben tomar decisiones acerca del uso que se le puede dar a la información, incluyendo las reglas del negocio. Los Propietarios son responsables de seleccionar los sistemas informáticos apropiados y los controles pertinentes para la información manejada por estos sistemas, consistente con las políticas y las normas establecidas por el departamento de Seguridad Informática [se puede insertar aquí un vínculo Intranet]. Por ejemplo, los Propietarios deben definir las reglas de validación utilizadas para verificar la exactitud y la aceptabilidad de los datos de entrada. Estas reglas de validación y los demás controles para la protección de la información deben ser autorizados formalmente por escrito por el Propietario correspondiente, antes de que se realicen modificaciones mayores a los sistemas de aplicaciones de producción. Los Propietarios deben entender los usos y los riesgos asociados con la información por la cual responden. Esto significa que son responsables de las consecuencias asociadas con divulgaciones inadecuadas, mantenimiento insuficiente, etiquetado incorrecto de la clasificaciones y otras deficiencias de control relacionadas con seguridad pertenecientes a la información para la que han sido designados Propietarios.

Roles y Responsabilidades de los Custodios—Los Custodios de la información son individuos, a menudo personal del departamento de Seguridad Informática o administradores de sistemas de departamentos locales, en posesión lógica o física de la información proveniente de los Propietarios. Los Custodios están encargados de suministrar los servicios de sistemas informáticos de acuerdo con las instrucciones de los Propietarios, incluyendo medidas de seguridad informática como el cifrado. A través del uso de sistemas de control de acceso lógicos y físicos, los Custodios deben proteger la información confiada a ellos de la distribución, acceso, modificaciones, destrucción o usos no autorizados. Los Custodios son también responsables por el suministro y la administración general de los respaldos y los sistemas de recuperación en concordancia con las políticas y normas emitidas por el departamento de Seguridad Informática. Los Custodios son los responsables de establecer, monitorear y manejar los sistemas informáticos de una manera consistente con las políticas y normas emitidas por el departamento de Seguridad Informática [un vínculo con estas políticas puede insertarse aquí]. Los Custodios deben suministrar reportes a los Propietarios periódicamente, en cuanto a los recursos consumidos en las actividades de los usuarios. Los Custodios no deben cambiar la información de producción que ellos poseen, a menos que hayan recibido un permiso temporal explícito del Propietario o del usuario autorizado.

Roles y Responsabilidades de los Usuarios—Los usuarios de la información son personas a quienes se ha otorgado autorización explícita para tener acceso, modificar, borrar o utilizar la información por parte del Propietario correspondiente. Los usuarios sólo deben utilizar la información para los fines específicamente autorizados por el Propietario. Los usuarios no pueden realizar copias adicionales o reproducir o diseminar información confidencial a menos que el Propietario esté de acuerdo. Los usuarios también deben cumplir todas las medidas de seguridad definidas por el Propietario, puestas en práctica por el custodio o definidas por el departamento de Seguridad Informática. Los usuarios, además, no pueden divulgar información que posean, a menos que ésta haya sido definida como pública, sin permiso del Propietario [un vínculo con la política de divulgación se puede insertar aquí]. Los usuarios deben informar al departamento de Seguridad Informática sobre cualquier situación donde crean que pueda existir una vulnerabilidad o violación a la seguridad [un vínculo al Centro de Atención al Usuario o algún otro mecanismo de ayuda se puede insertar aquí]. La gerencia local debe proporcionar suficiente tiempo a los usuarios para ser adiestrados en cuanto a

seguridad, y los usuarios deben asistir a tales adiestramientos de manera periódica. Los usuarios de computadores personales tienen responsabilidades especiales, por ejemplo, en relación con los respaldos y al rastreo de virus, que son definidos en la Política de Seguridad de Computador Personal [un vínculo Intranet con dicho documento se puede insertar aquí].

Múltiples Roles y Responsabilidades—Es posible que ciertas personas tengan responsabilidades multidisciplinarias en relación con cierto tipo de información. Por ejemplo, un empleado puede ser el generador de un nuevo tipo de información de producción que está almacenada en un computador personal. En este caso, el trabajador debe, al menos temporalmente, actuar como Propietario, Custodio y Usuario. Para lograr un ambiente operacional más seguro, diferentes personas deben ejercer los roles de Propietario, Custodio y usuario cada vez que la información de producción tenga más de un usuario. Los generadores de nuevos tipos de información de producción deben informar inmediatamente al grupo de Arquitectura de Sistemas Informáticos dentro del departamento de Tecnología Informática, de modo de establecer y mantener los roles y responsabilidades correspondientes.

Designación de Propietarios—De existir varios Propietarios potenciales de la información, el director de informática debe asignar la responsabilidad de propiedad al gerente ejecutivo del negocio que tiene el mayor uso de la información. Cuando se tiene el rol de Propietario, la persona debe tomar en consideración las necesidades e intereses de otros accionistas que se apoyen o tengan interés en la información. Con excepción de la información operativa sobre los computadores y las redes, los gerentes del departamento de Seguridad Informática no deben ser Propietarios de ninguna información. El rol y la responsabilidad como Propietario deben ser delegadas a cualquier gerente de tiempo completo en la unidad de negocios del Propietario. Los roles y las responsabilidades del Propietario no pueden ser asignados o delegados a contratistas, consultores o a personas de organizaciones externas al negocio o servicios externos.

Designación de Custodios—La gerencia debe asignar responsabilidades específicas para las medidas de control que protegen cada tipo principal de información de producción [aquí puede insertarse un vínculo a un diccionario corporativo de datos que defina estos tipos de información]. Los Propietarios tienen la responsabilidad de identificar a todos aquellos individuos que están en posesión de la información y de la cual han sido designados Propietarios. Estos individuos se convierten en Custodios de manera automática. Aunque se debe

prestar especial atención a los roles y responsabilidades relacionados con la seguridad cuando estén involucrados individuos externos, se puede permitir que un Custodio sea un contratista, consultor, o un individuo perteneciente a una organización externa.

Designación de Usuarios—Los usuarios pueden ser empleados, empleados temporales, contratistas, consultores o terceros con quienes se haya llegado a arreglos especiales, tales como los acuerdos de confidencialidad, [se puede insertar aquí un vínculo con un formato de confidencialidad]. Los Propietarios deben conocer a todos los usuarios y todos deben recibir de éste una autorización. Las actividades relevantes de seguridad de todos los usuarios deben tener un seguimiento y ser registradas por el Custodio. Los usuarios deben ser siempre personas específicas. Los usuarios no deben ser definidos como departamentos, equipos de proyecto u otros grupos.

Cambios de Condición—Las personas variarán en sus roles de Propietarios, Custodios y usuarios de información. Es responsabilidad del gerente local informar rápidamente los cambios de condición al departamento corporativo de Recursos Humanos. Tan pronto se conozcan, los cambios en la condición deben reflejarse inmediatamente en la base de datos del departamento corporativo de Recursos Humanos. Estos cambios en la condición del trabajador, serán automáticamente comunicados al departamento de Seguridad Informática y a los administradores de los sistemas locales. Los Custodios deben mantener los sistemas de control de acceso de modo que los privilegios de usuario previamente otorgados no se vuelvan a otorgar, cada vez que ocurra un cambio en la condición del usuario. Cuando un Custodio tenga un cambio de condición, es responsabilidad del Propietario asignar rápidamente un nuevo Custodio, y ayudar al nuevo Custodio en sus nuevas tareas, incluyendo el adiestramiento necesario. Cuando un Propietario tenga un cambio de condición, es responsabilidad del director de informática el designar rápidamente a un nuevo Propietario [una lista de los Propietarios podría aparecer en el diccionario corporativo de datos accesible a través de Intranet y un vínculo a dicha página podría suministrarse aquí].

Manejo de la Información Despues de Cambios en la Condición—Los usuarios que cambien su condición deben dejar toda la información de producción con su gerente inmediato. Tan pronto ha habido un cambio en la condición del usuario, su gerente inmediato debe revisar tanto los archivos residentes en los computadores como los archivos de documentos, a fin de determinar quién debe ser el Propietario de los archivos, o los métodos apropiados a utilizar para la eliminación o

destrucción de los archivos. El gerente rápidamente debe re-asignar las tareas de los usuarios y específicamente delegar responsabilidad de la información que estaba en manos del usuario anterior. Es responsabilidad del gerente adiestrar al nuevo usuario de modo que éste pueda realizar totalmente las labores realizadas por el usuario anterior. Es responsabilidad de este gerente familiarizar al nuevo usuario con las relaciones personales que el usuario anterior mantenía con entes internos y externos, y con todas las transacciones pendientes y los proyectos incompletos manejados por el usuario anterior.

Revisión Periódica de la Lista de Privilegios—Cada trimestre calendario, el departamento de Seguridad Informática debe suministrar a los Propietarios una lista de los usuarios autorizados para acceder a la información de la cual dichos Propietarios son responsables. Dentro de los 10 días hábiles siguientes a la recepción de dicha lista, los Propietarios deben devolver al departamento de Seguridad Informática su autorización de todos los permisos vigentes otorgados a los usuarios de la información para la cual ellos son los Propietarios designados, y cualquier corrección o eliminación que sea necesaria.

Información Suministrada desde el Exterior—En el curso de actividades normales del negocio, la Empresa X a menudo toma posesión de la información confidencial de terceros. Cada vez que se haya firmado un acuerdo de confidencialidad (NDA, por sus siglas en inglés), se debe designar un Propietario interno de la Empresa X para la información así recibida [un vínculo con este tipo de NDA se puede insertar aquí]. El gerente de la unidad de negocios que utiliza la información es a menudo designado Propietario. El Propietario debe informar rápidamente la existencia de la información de este tercero al grupo de Arquitectura Informática del departamento de Tecnología Informática para incluirlo en el diccionario corporativo de datos [un vínculo al formato que reporte sobre dicha información se puede insertar aquí]. Esta información de terceros se debe etiquetar con la categoría de clasificación de datos apropiada, y se debe tratar como si fuera información interna de la Empresa X con la misma clasificación [un vínculo a la política de clasificación de datos se puede insertar aquí]. Los roles y responsabilidades para los Custodios y usuarios son también pertinentes a la información suministrada externamente.

Diccionario de Datos Corporativo—Para ayudar en el manejo de la información, el departamento de sistemas informáticos debe recopilar y actualizar anualmente un diccionario de datos corporativo y otras descripciones de alto nivel de los activos principales de información

de la Empresa X residentes en los sistemas de producción. Es responsabilidad del director de información asegurarse de que este diccionario de datos incluya una nota informativa vigente acerca de quiénes son los Propietarios actuales de los activos informáticos de producción de la Empresa X. Es responsabilidad de todos los Propietarios conocer la identidad de los Custodios y usuarios de los tipos de información que han sido confiados a su cuidado.

Rol de Apoyo del Grupo de Arquitectura Informática—Aunque no esté directamente involucrado con los Propietarios, los Custodios y los usuarios en su diario manejo de la información, el grupo de Arquitectura Informática del departamento de Tecnología Informática es responsable del desarrollo y mantenimiento de la arquitectura informática de una empresa. El grupo de Arquitectura Informática es también responsable de la generación y mantenimiento de un diccionario de datos corporativo, incluyendo las definiciones adecuadas para varios tipos de información de producción. El Grupo de Arquitectura Informática es además responsable de construir una base de datos que hace seguimiento de las personas que desempeñan los roles de Propietario y Custodios. Conjuntamente con el departamento de Seguridad Informática, el grupo de Arquitectura Informática tiene la responsabilidad adicional de fomentar el compartir la información de la Empresa X de manera eficiente y con la seguridad adecuada.

Sistema de Registro—Cada Propietario debe designar un sistema de registro que debe servir de copia de mayor nivel de confiabilidad de la información bajo su cuidado. Se deben llevar a cabo actualizaciones de esta información en los sistemas de registro antes o durante las actualizaciones a diferentes sistemas contentivos de

la misma información. Es responsabilidad del Propietario garantizar que toda las copias de producción de la información para las cuales ha sido designado Propietario, mantengan los controles apropiados para asegurar un mínimo de exactitud, disponibilidad e integridad.

Proceso de Aceptación del Riesgo—Pocas veces se permitirán excepciones a las políticas y normas de seguridad informática, pero sólo si el Propietario de la información, el director del departamento de Seguridad Informática y el director de información han firmado un formulario de aceptación del riesgo. En ausencia de tal autorización por parte de la gerencia y reflejada en un formulario de aceptación de riesgo, todos los Propietarios, los Custodios y los usuarios deben observar constantemente las políticas y normas de seguridad informática de la Empresa X.

Notificación de Pérdida o Divulgación—Si se extravía o divulga información confidencial a terceros no autorizados, o si existe la sospecha de pérdida o divulgación a terceros no autorizados de dicha información, se debe notificar inmediatamente a su Propietario y al director del departamento de Seguridad Informática.

Aprobado por: [insertar el nombre del ejecutivo encargado de la autorización]

Fecha de aprobación: DD/MM/AA.

Fecha de Vigencia: DD/MM/AA.

Versión Número: XX



Capítulo 20 MODELO DE POLÍTICA DE CORTAFUEGOS

Objetivo y Alcance de la Política—Los cortafuegos constituyen un componente esencial de la infraestructura de seguridad de los sistemas informáticos de la Empresa X. Los cortafuegos se pueden definir como sistemas de seguridad que controlan y restringen la conexión entre redes y los servicios de dichas redes. Los cortafuegos establecen un punto de control en el cual se pueden aplicar los controles de acceso. La conectividad define a cuáles sistemas de computación se permite intercambiar información. A un servicio también se le puede denominar aplicación, y se refiere a la manera en que la información fluye a través del cortafuego. Ejemplos de servicios incluyen el protocolo de transferencia de archivos (FTP) y exploración en la Web (HTTP). Esta política define las reglas esenciales relacionadas con la administración y mantenimiento de los cortafuegos de la Empresa X y se aplica a todos los cortafuegos que sean de su propiedad, alquilados, alquilados con opción a compra o controlados por los empleados de la Empresa X.

El Papel del Cortafuego—En algunas instancias, sistemas tales como enruteadores, interfaces de telecomunicaciones o puertas de enlace, pueden funcionar como cortafuegos aun cuando formalmente no sean cortafuegos. Todos los sistemas de la Empresa X que actúan como cortafuegos, bien sea que reciban este nombre o no, deben ser manejados de conformidad con las reglas definidas en esta política. En algunas instancias, esto requerirá que los sistemas se actualicen para sustentar la funcionalidad mínima definida en esta política.

Aplicabilidad de la Política—Todos los cortafuegos de las redes de la Empresa X, manejados bien sea por empleados o por terceros, deben seguir esta política. Evadir esta política sólo será permitido mediante previa autorización por escrito del gerente de Seguridad Informática.

Documentación Requerida—Antes de instalar y usar cualquier cortafuego de la Empresa X, se debe entregar al gerente de Seguridad Informática un diagrama con las vías permitidas, con una justificación para cada una de ellas, y una descripción de los servicios permitidos conjuntamente con una justificación para cada uno. El permiso para lograr tales vías y servicios será otorgado por el gerente de Seguridad Informática, sólo cuando estas vías o servicios sean necesarios por razones importantes de negocios, y se empleen consistentemente

suficientes medidas de seguridad. La conformidad del despliegue de los cortafuegos con la documentación suministrada será revisada eventualmente por el departamento de Auditoría Interna. Cualquier cambio de las vías o de los servicios debe pasar por el mismo proceso descrito a continuación.

Negación Predeterminada—Toda vía de conexión y servicio que no esté específicamente permitida por esta política y por los documentos que la sustenten, emitidos por el departamento de Seguridad Informática, debe ser bloqueada por los cortafuegos de la Empresa X. La lista de las vías y de los servicios recientemente autorizados debe ser documentada y distribuida a todos los administradores de sistemas y bajo el conocimiento del departamento de Seguridad Informática. El departamento de Seguridad Informática debe mantener un inventario de todas las vías de acceso dentro y fuera de la red de la Empresa X.

Conexiones Entre Máquinas—No deben establecerse o activarse conexiones en tiempo real entre dos o más sistemas de computación de la Empresa X, a menos que el departamento de Seguridad Informática determine que tales conexiones no dañarán la seguridad de la información. En muchos casos se deben emplear cortafuegos o sistemas intermedios similares. Este requisito se aplica sin importar la tecnología empleada, inclusive conexiones inalámbricas, enlaces a través de microondas, módem por cable, redes digitales de servicios integrados, así como líneas de conexión digitales para suscriptores. Cualquier conexión entre el sistema de producción interno de la Empresa X y cualquier sistema de computación externo o cualquier red externa de computación o proveedor de servicios, debe ser autorizado de antemano por el departamento de Seguridad Informática.

Realización de Pruebas Periódicas—Debido a que los cortafuegos suministran una medida de control tan importante para la red de la Empresa X, su fortaleza y su configuración apropiada debe ser puesta a prueba periódicamente. Si los proveedores de software lo respaldan, estas pruebas deben incluir la utilización de agentes de software que automáticamente revisen si los cortafuegos mantienen su configuración y operan de una manera consistente tanto con las políticas de seguridad de la Empresa X como con el grupo de Arquitectura de Seguridad Informática de la Empresa X. Este proceso de prueba debe incluir la consideración de los parámetros

de configuración definidos, los servicios permitidos, las vías de conexión permitidas, las prácticas vigentes de administración y la adecuación de las medidas de seguridad empleadas. Estas pruebas deben incluir la ejecución periódica de software de identificación de vulnerabilidades y la realización regular de pruebas de penetración. Estas pruebas deben ser ejecutadas por personas técnicamente preparadas bien sea en el departamento de Auditoría Interna o empleados de un contratista. Los responsables de la administración o del manejo de los cortafuegos correspondientes no deben realizar estas pruebas.

Registros—Todos los cambios realizados en los parámetros de configuración de los cortafuegos, así como en los servicios y conexiones permitidas deben quedar registrados. Cualquier actividad sospechosa que pueda indicar el uso no autorizado o intento de comprometer las medidas de seguridad debe también quedar registrada. La integridad de estos registros debe estar protegida con sumas verificadoras, firmas digitales, cifrados o medidas parecidas. Estos registros se deben eliminar rápidamente de los sistemas de registros y almacenarse en un contenedor físicamente protegido por lo menos durante seis meses después de la fecha en que fueron grabados. Estos registros se deben revisar periódicamente para garantizar que los cortafuegos están funcionando de manera segura.

Detección de Intrusiones—Todos los cortafuegos de la Empresa X deben incluir sistemas de detección de intrusiones, autorizados por el departamento de Seguridad Informática. Cada uno de estos sistemas de detección de intrusiones debe estar configurado de conformidad con las especificaciones definidas por el departamento de Seguridad Informática. Entre otros problemas potenciales, estos sistemas de detección de intrusiones deben detectar modificaciones no autorizadas a los archivos del sistema de los cortafuegos y detectar ataques actuales de denegación de servicios. Tales sistemas de detección de intrusiones deben notificar inmediatamente, a través de buscapersonas, al personal técnico que pueda ejercer acciones correctivas. Todo el personal técnico que trabaje con cortafuegos debe tener acceso a sistemas remotos y contar con privilegios con los que puedan responder inmediatamente a estos incidentes, aun cuando no estén físicamente presentes.

Planificación de Contingencias—El personal técnico que trabaje con cortafuegos debe preparar y obtener la autorización del departamento de Seguridad Informática, para planes de contingencias que orienten las acciones a tomar en caso de varios problemas, inclusive la puesta en peligro del sistema, averías en el

sistema, fallas en el sistema, sobrecargas y la suspensión del servicio de Internet. Estos planes de contingencia se deben poner a prueba para que reflejen los cambios en el ambiente de los sistemas informáticos de la Empresa X. Estos planes de contingencia se deben poner a prueba periódicamente para garantizar que serán efectivos en la restauración de un ambiente informático confiable y seguro.

Conexiones Externas—Todas las conexiones entrantes de Internet en tiempo real a las redes internas de la Empresa X o sistemas de computación multiusuario deben pasar a través de un cortafuego antes de que los usuarios reciban el mensaje de bienvenida para acceder al sistema. Aparte de los computadores personales (PC) que acceden a Internet sobre una base de discado saliente por sesión individual, ningún sistema de computación de la Empresa X puede estar conectado con Internet a menos que esté protegido por un cortafuego. Los sistemas de computación que requieren protección de cortafuegos incluyen los servidores web, servidores de comercio electrónico y servidores de correo. Todos los computadores personales con línea digital de suscriptor o con conexión de módem por cable, deben utilizar un cortafuego autorizado por el departamento de Seguridad Informática. Siempre que el cortafuego lo sustente, la pantalla de acceso debe tener un aviso que indique que al sistema sólo pueden acceder usuarios autorizados, y los que inicien una sesión es porque están autorizados para hacerlo, que el uso no autorizado del sistema o el abuso están sujetos a acciones disciplinarias, inclusive medidas judiciales y que el uso del sistema será monitoreado y registrado.

Autentificación Extendida de Usuario—El tráfico entrante, con excepción del correo electrónico de Internet, la distribución de noticias y transmisiones forzadas previamente autorizadas por el departamento de Seguridad Informática, que tienen acceso a la red de la Empresa X a través de un cortafuego, debe mantener en toda circunstancia medidas de autentificación extendida de usuario, autorizadas por el departamento de Seguridad Informática. Ejemplos de sistemas de autentificación extendida de usuario incluyen las contraseñas dinámicas y los certificados digitales.

Redes Privadas Virtuales—Para evitar la divulgación no autorizada de información confidencial y valiosa, todo el tráfico entrante, con excepción del correo de Internet, los servicios de noticias autorizadas, y las transmisiones forzadas que tienen acceso a las redes de la Empresa X, se debe cifrar con los productos autorizados por el departamento de Seguridad Informática [se puede insertar aquí un vínculo a la lista de productos autorizados]. Estas conexiones a menudo se denominan

redes privadas virtuales (VPN, por sus siglas en inglés). Las VPN autorizadas en las redes de la Empresa X, combinan la funcionalidad de la autenticación extendida de usuario con la funcionalidad de las comunicaciones cifradas [se puede insertar aquí un vínculo a la página Intranet con información de productos sobre seguridad informática].

Mecanismos de Acceso a los Cortafuegos—Todos los cortafuegos de la Empresa X deben tener una contraseña única u otros mecanismos de control de acceso. La misma contraseña o el mismo código de control de acceso no debe ser utilizado en más de un cortafuego. Cada vez que cuenten con el apoyo del proveedor de los cortafuegos correspondientes, los que administran los cortafuegos de la Empresa X deben tener su identidad vigente a través de mecanismos de autenticación extendida de usuario. En algunos ambientes de mayor seguridad, designados por el gerente de Seguridad Informática, tal como el sitio de comercio de Internet de la Empresa X, el acceso remoto a los administradores de los cortafuegos está prohibido. Todas las actividades de administración de cortafuegos deben ser llevadas a cabo personalmente y en el sitio.

Privilegios de Acceso a los Cortafuegos—Los privilegios para modificar la función, la conexión y los servicios sustentados por los cortafuegos se deben restringir a unas pocas personas con adiestramiento técnico con necesidad de dichos privilegios. A menos que el gerente de Seguridad Informática emita la autorización correspondiente, estos privilegios sólo deben otorgarse a aquellas personas que sean empleados permanentes de la Empresa X, y no a empleados temporales, contratistas, consultores o personal en empresas externas. Todos los cortafuegos deben contar con por lo menos dos integrantes del personal con adiestramiento adecuado para realizar cambios, según lo requieran las circunstancias. Tal adiestramiento incluye un curso de actualización de conocimientos o la asistencia a conferencias que permita a los miembros del personal mantenerse al día con los últimos avances en tecnología y operaciones de cortafuegos. Debe darse especial atención a la elaboración de cronogramas de vacaciones fuera de la ciudad, de manera que al menos uno de los integrantes del personal de administración de los cortafuegos esté disponible todo el tiempo.

Subredes Aseguradas—Partes de la red interna de la Empresa X que contiene información valiosa y confidencial, tales como los computadores utilizados por el departamento de Recursos Humanos, deben utilizar una subred asegurada. El acceso a ésta y otras subredes debe restringirse con cortafuegos y otras medidas de control de acceso. Basado en evaluaciones

periódicas de riesgos, el departamento de Seguridad Informática definirá las subredes de seguridad necesarias en la Arquitectura de Seguridad Informática.

Zonas Desmilitarizadas—Todos los servidores comerciales de Internet inclusive los servidores de pago, los servidores de bases de datos y los servidores web, deben estar protegidos por cortafuegos y ubicados dentro de una zona desmilitarizada (DMZ, por sus siglas en inglés), una subred que esté protegida de Internet por uno o más cortafuegos. Una red de trabajo interna, tal como Intranet, está también protegida de la subred DMZ por uno o más cortafuegos.

Sistemas de Administración de Redes—Los cortafuegos deben estar configurados de tal manera que sean visibles a los sistemas internos de administración de redes. Los cortafuegos también deben estar configurados para permitir el uso de herramientas remotas para auditorías automáticas a ser utilizadas por los integrantes autorizados del personal de la Empresa X. A menos que se utilicen deliberadamente en pruebas, tales herramientas automáticas para auditorías no deben iniciar una secuencia de respuestas a través de sistemas de detección de intrusiones conectados a cortafuegos.

Divulgación de Información Interna de las Redes—Las direcciones, las configuraciones, los productos empleados y la información del diseño de los sistemas internos correspondientes al sistema de computación y redes de la Empresa X, se deben restringir de tal manera que tanto los sistemas como los usuarios externos a la red interna de la Empresa X no tengan acceso a esta información.

Respaldo Seguro—Las copias vigentes fuera de línea de los archivos de configuración de los cortafuegos, los archivos de permisos de conectividad, los archivos de documentación procedimental para la administración de sistemas de cortafuegos y los archivos correspondientes, se deben guardar todo el tiempo cerca del cortafuego. Una alternativa posible para copias sin conexión implica versiones cifradas de estos mismos archivos. Donde lo permitan los sistemas de software, se debe continuar con el restablecimiento automático de las copias autorizadas de estos archivos de sistemas, cada vez que se detecte una modificación no autorizada a dichos archivos.

Rastreo de Virus y Contenido—El software antivirus autorizado por el departamento de Seguridad Informática se debe instalar y activar en todos los cortafuegos de la Empresa X. Debido a que los archivos que pasan a través de los cortafuegos pueden estar cifrados o comprimidos, los sistemas antivirus instalados en cortafuegos pueden no detectar todos los

archivos infectados por virus. Por este motivo, el software antivirus se requiere en todos los servidores de correo de la Empresa X, en los servidores departamentales y en los computadores personales. Tanto el software para el filtrado de contenido como el software que impide que los usuarios puedan acceder a ciertos sitios de la red que no tienen que ver con el negocio, deben estar activados también en todos los cortafuegos de la Empresa X.

Cortafuegos Dedicados—Los cortafuegos deben funcionar en máquinas dedicadas que no realicen ningún otro servicio, como el de servidor de correo. La información crítica o confidencial de la Empresa X no debe estar nunca almacenada en un cortafuego. Tal información puede ser mantenida en memoria intermedia a medida que atraviesa los cortafuegos. Los cortafuegos deben contener un mínimo de software de sistema operativo activo. Donde lo permita el sistema operativo de respaldo, todos el software que no se utilice y resulte innecesario se debe eliminar del cortafuegos. La Empresa X no permite que su información interna resida o se procese a través de cualquier cortafuego, servidor u otro computador que comparta con otra organización en una instalación externa. Están permitidos los enrutadores, los concentradores, los módem y otros componentes de la red suministrados por organizaciones externas

Controles en Modificaciones a Cortafuegos—Debido a que sustentan las actividades de los sistemas informáticos críticos de la Empresa X, los cortafuegos se consideran sistemas de producción. El gerente de Seguridad Informática debe autorizar previamente todos los cambios del software suministrado por proveedores, excepto las actualizaciones y los parches que suministran dichos proveedores. La misma documentación que se requiere para modificaciones en los sistemas de producción se debe preparar para los cortafuegos.

Publicación de Actualizaciones—Los cortafuegos de la Empresa X deben ejecutar la última versión de software para impedir estos ataques. Si están disponibles, todos los cortafuegos de la Empresa X deben estar suscritos a servicios de software de mantenimiento y de actualización. A menos que esté autorizado con anterioridad por el gerente de Seguridad Informática, los integrantes del personal que tengan la responsabilidad

del manejo de los cortafuegos, deben instalar y activar estas actualizaciones dentro de los dos días hábiles siguientes a su recepción.

Monitoreo de Vulnerabilidades—Los integrantes del personal de la Empresa X que tengan la responsabilidad del manejo de los cortafuegos, se deben suscribir al Equipo de Respuesta ante Emergencias en Computadores y a otras fuentes importantes que suministren información vigente acerca de las vulnerabilidades de los cortafuegos. El departamento de Seguridad Informática debe estar atento a cualquier vulnerabilidad que afecte las redes y los sistemas de la Empresa X.

Productos Autorizados—A menos que se obtenga una autorización escrita con anterioridad por parte del gerente de Seguridad Informática, sólo aquellos cortafuegos que aparezcan en la lista de proveedores y productos autorizados se podrán desplegar en las redes de la Empresa X [inserte un vínculo a la lista de productos autorizados]. Todas las interfaces y características de los cortafuegos, como el rastreo de virus, deben ser consistentes con la Arquitectura de Seguridad Informática emitida por el departamento de Seguridad Informática.

Seguridad Física del Cortafuego—Todos los cortafuegos de la Empresa X se deben ubicar en sitios cerrados y estar accesibles sólo a los que llevan a cabo tareas de mantenimiento y actualización de los mismos, así autorizados por la gerencia del departamento de Tecnología Informática. Está prohibido la ubicación de un cortafuego en un área abierta dentro de un centro de procesamiento de datos, pero es admisible, su ubicación en sitios diferentes y cerrados aunque estén dentro de un centro de procesamiento de datos generales. Estos sitios deben estar equipados con alarmas y un registro automático de todas las personas que tengan acceso a esa sala.

Aprobado por: [inserte el nombre del ejecutivo que autoriza]

Fecha de aprobación: DD/MM/AA.

Fecha de vigencia: DD/MM/AA.

Número de la versión: XX



Apéndice A

LISTA DE REFERENCIAS PARA LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Se recomienda la siguiente lista de referencias suplementarias como material de consulta al redactar políticas originales o realizar el mantenimiento de las existentes.

Acceso, Uso y Divulgación del Correo Electrónico en los Sistemas Informáticos de la Empresa: Un Kit de Herramientas para Formular la Política de su Empresa. Electronic Messaging Association, Arlington, VA. 1996.

Lista de Verificación de Prácticas Responsables en el Manejo de la Información. Privacy Rights Clearing House, Universidad de San Diego, Center for Public Interest Law, Fact Sheet #12, January 1995.

Cobb, Steven. *Guía de Políticas de Cortafuegos NCSA.* National Computer Security Association, Carlisle, PA. 1996. www.ncsa.com

Código de Prácticas para la Gestión en Seguridad Informática. British Standards Institution, Departamento de Comercio e Industria. Gobierno Británico. Londres, Inglaterra. 1995 (segunda edición). También se conoce como BS 7799.

Corby, Michael, y Robert E. Johnston. "Lineamientos de Seguridad en Intranet: Cómo Proteger la Empresa a Medida Que Crece la Intranet," *Computer Security Journal*, vol. XIV, no. 4, 1998.

Datapolítica: Seguridad Informática en Países Nórdicos. Consejo de Ministros Nórdicos, Kobenhavn, Dinamarca. 1993.

Manual en Borrador de las Naciones Unidas sobre el Delito Computarizado. Departamento Canadiense de Justicia, Otawa, Canadá. Septiembre 1992.

Lista de Verificación de Prácticas Informáticas Aceptables. Direct Marketing Association, New York, NY. 1992.

Manual de Prácticas Informáticas Aceptables. Direct Marketing Association, New York, NY. 1994.

Gilbert, Gregory A. "Cómo Desarrollar una Política de Seguridad en Computación", *Reportes Datapro sobre Seguridad Informática.* McGraw-Hill. Enero 1989.

Gritzalis, Dimitris. "Una Política de Seguridad de Línea de Base para los Sistemas Informáticos Distribuidos en el Área de la Salud", *Computers & Security*. vol. 16, no. 8, pp. 709-719. 1997.

Lineamientos para Establecer Políticas de Seguridad Informática en Organizaciones Que Utilizan Sistemas de Registros de Pacientes Basados en Computadores, Febrero 1995. Computer-based Patient Record Institute Inc., 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173 USA. Tel. 708-706-6746.

Lineamientos para Programas de Educación en Seguridad Informática en Organizaciones Que Utilizan Sistemas de Registros de Pacientes Basados en Computadores, Junio 1995. Computer-based Patient Record Institute Inc., 1000 E. Woodfield Road, Suite 102, Schaumburg, IL 60173 USA. Tel. 708-706-6746.

Lineamientos sobre Protección de Registros Médicos En Línea, 1996. American Health Information Management Association, 919 N. Michigan Ave., Suite 1400, Chicago, IL 60611-1683 USA. Tel. 312-787-2672.

Uso de Internet y la Plantilla de Seguridad. On Technology Corporation. Cambridge, MA. 1997. www.on.com

Lindup, Kenneth. "Un Nuevo Modelo para las Políticas de Seguridad Informática", *Computers & Security*. vol. 14, pp. 691-695. 1995.

Overbeek, Paul, Wim Sipman, y Leon Strous. *Manual de Normas en Seguridad Informática.* 1994. Kluver Academic Publishers. Dordrecht, Holanda. Fax 078-334911.

Ozier, Will. *Principios Generalmente Aceptados en Seguridad de Sistemas (PGASS).* Exposure Draft 2.0. Information Systems Security Association. Chicago, IL. November 1995. www.ibm.com/security/wpconsul.htm

Page, Stephen B. *Establecimiento de un Sistema de Políticas y Procedimientos.* Page Publishing. Westerville, Ohio. 1998.

Ruthberg, Zella G. y Harold F. Tipton. *Manual de Gestión de la Seguridad Informática.* Auerbach Publishers. Boston, MA. 2000.

Schweitzer, James. "Clasificación de la Información para Efectos de Seguridad," *Reportes DataPro Sobre la Seguridad Informática*. IS15-250-101. Enero 1989.

Wood, Charles Cresson. "Establecimiento de Normas Internas de Seguridad para los Sistemas Técnicos", *Computers & Security* (UK). pp. 193-200. Elsevier. Oxford, Inglaterra. Agosto 1986.

Wood, Charles Cresson. *Roles y Responsabilidades en Seguridad Informática*. PentaSafe Security Technologies, Inc. Houston, Texas. 2001.

Wood, Charles Cresson. "Principios de Diseño de Sistemas Informáticos Seguros", *Computers & Security* (UK). vol. 9, no. 1, pp. 13-24. Elsevier. Oxford, Inglaterra. Febrero 1990.

Wright, Benjamin. *La Ley del Comercio Electrónico: EDI, Fax, y E-Mail—Tecnología, Prueba y Responsabilidad*. Little, Brown and Company. Boston, MA. 1991.



Apéndice B

LISTA DE PUBLICACIONES PERIÓDICAS SOBRE SEGURIDAD INFORMÁTICA

2600: The Hacker Quarterly—Revista y boletín clandestino publicados por un hacker. P.O. Box 752, Middle Island, NY 11953-0752 USA; teléfono (631) 751-2600; fax (631) 474-2677; www.2600.com and 2600@well.sf.ca.us

Cipher: Newsletter of the Technical Committee on Security & Privacy—Un boletín con artículos de ingeniería orientados a la investigación. Institute of Electrical and Electronics Engineers (IEEE) Computer Society, Code 5540, Naval Research Laboratory, Washington, DC 20375-5337 USA; teléfono (202) 404-7931; fax (202) 404-7942; www.ieee-security.org/cipher.html y cipher@issl.iastate.edu

Computer Fraud & Security—Un boletín informativo que trata sobre los últimos delitos de computación y consejos prácticos para la gerencia. Elsevier Science, 655 Avenue of the Americas, New York, NY 10010-5107 USA; teléfono +1-212-633-3730; fax +1-212-633-3680; www.elsevier.com y usinfo-f@elsevier.com

Computer Law & Security Report—Un análisis legal sobre problemas recientes de alta tecnología y qué hacer al respecto, dirigido a abogados y especialistas en seguridad informática. Elsevier Science, 655 Avenue of the Americas, New York, NY 10010-5107 USA; teléfono +1-212-633-3730; fax +1-212-633-3680; www.elsevier.com y usinfo-f@elsevier.com

Computer Professionals For Social Responsibility Newsletter—Una revisión ética de recientes acontecimientos relacionados con seguridad informática, particularmente la privacidad y asuntos de libertad. Computer Professionals For Social Responsibility; PO Box 717, Palo Alto, CA 94302-0717 USA; teléfono (650) 322-3778; fax (650) 322-4748; www.cpsr.org y djlin@quark.cpsr.org

Computers & Security—Una publicación internacional de investigación de seguridad informática que registra acontecimientos novedosos en el campo de la seguridad informática, abocada a investigaciones recientes. Elsevier Science, 655 Avenue of the Americas, New York, NY 10010-5107 USA; teléfono +1-212-633-3730; fax +1-212-633-3680; www.elsevier.com y usinfo-f@elsevier.com

Computer Security Alert—Un boletín informativo que brinda consejos prácticos y experiencia de otros practicantes en el campo de la seguridad informática. Computer Security Institute (División de CMP), 600 Harrison St., San Francisco, CA 94107 USA; teléfono (415) 947-6320, fax (415) 947-6023; www.goci.com y csci@cmp.com

Computer Security Journal—Un diario que publica estudios de casos y artículos de personas con experiencia. Computer Security Institute, 600 Harrison St., San Francisco, CA 94107 USA; teléfono (415) 947-6320; fax (415) 947-6023; www.goci.com; csci@cmp.com

Contingency Planning & Management—Una publicación que trata sobre asuntos de gerencia asociados con sistemas informáticos y otros tipos de planificación de contingencias. Witter Publishing Company, 84 Park Ave., Flemington, NJ 08822 USA; teléfono (908) 788-0343; fax (908) 788-3782; www.contingencyplanning.com y cpmmagazine@witterpublishing.com

Cyber Security Advisor—Un boletín informativo acerca de los nuevos desarrollos en el campo de seguridad informática. Advisor Media (división de Aspen Publishers), 7201 McKinney Circle, Frederick, MD 21704 USA; teléfono (858) 278-5600; www.cybersecurityadvisor.com

Cybertek—Una revista que trata de supervivencia y tecnología combinada con anti-seguridad en computación (material de archivo solamente). Cybertek Magazine, PO Box 64, Brewster, NY 10509 USA; www3.l0pht.com/~oblivion//cybertek/cybertek.html

Disaster Recovery Journal: The Journal Dedicated to Corporate Disaster Recovery Planning—Una publicación para los responsables de gerenciar, preparar o supervisar la planificación de contingencias (relacionadas con sistemas informáticos y similares). Systems Support, Inc., PO Box 510110, St. Louis, MO 63151 USA; teléfono (314) 894-0276; fax (314) 894-7474; www.drj.com and drj@drj.com

E-Business Advisor—Una publicación periódica que trata sobre estrategias y herramientas para comerciar en Internet. Advisor Media, 5675 Ruffin Road, Suite 200, San Diego, CA 92123 USA; teléfono (858) 278-5600; fax (858) 278-0300; www.advisor.com y order@advisor.com

EDPACS: The EDP Audit, Control & Security Newsletter—Un boletín informativo que cubre gran variedad de tópicos relacionados con seguridad computacional. CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431 USA; teléfono (800) 272-7737 ó (561) 994-0555; fax (800) 374-3401; www.crcpress.com

Emergency Preparedness Digest—Una revista que trata asuntos de planificación de contingencias, muchas relacionadas con computación. Emergency Preparedness Canada-Communications Directorate, 122 Bank Street, 2nd Floor, Ottawa, Ontario K1A 0W6 Canada; teléfono (613) 991-7077; fax (613) 996-0995; www.epc-pcc.gc.ca and opscen@ocipep-bpiepc.gc.ca

Emergency Preparedness News—Un boletín informativo dedicado a asuntos de planificación de contingencias incluyendo el manejo de crisis. Business Publishers, 8737 Colesville Rd., Ste. 1100, Silver Spring, MD 20910-9973 USA; teléfono (800) 274-6737 ó (301) 589-5103; fax (301) 587-4530; www.bpinews.com and stet@bpinews.com

FISSEA News and Views—Un boletín informativo sobre entrenamiento en seguridad informática importante para agencias gubernamentales. Federal Information Systems Security Educators' Association, c/o US Department of Commerce, National Institute of Standards & Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930 USA; <http://csrc.nist.gov/organizations/fisseam.html> y fisseamembership@nist.gov; teléfono (301) 975-2489; fax (301) 948-0279

Fraud Intelligence—Un boletín informativo sobre fraudes en Internet, tecnología sobre prevención de fraudes y técnicas de investigación. Informa Professional Publishers, Sheepen Place, Colchester, Essex CO3 3LP Reino Unido; teléfono +44 (0) 1206 772223; fax +44 (0) 1206 772771; www.informafinance.com/fi e informa.asia@informa.com

Frontline Solutions—Una revista sobre códigos de barra, reconocimiento de huellas digitales, reconocimiento óptico y tecnologías relacionadas. Advanstar Communications, Inc., 7500 Old Oak Blvd., Cleveland, OH 44130 USA; teléfono (440) 891-2766; fax (216) 723-9533; www.advanstar.com

Hack-Tic—Una revista holandesa que trata sobre hackers de computación y solo se accede a ella a través de la página Web. www.hacktic.nl

Information Executive—Un boletín informativo que trata sobre una variedad de tópicos incluyendo seguridad informática. Association of Information Technology Professionals (AITP), 315 South Northwest Highway, Suite 200, Park Ridge, IL 60068-4278 USA; teléfono (800) 224-9371 x226 or (847) 825-8124; fax (847) 825-1693; wwwAITP.org/publications/contents.html

Information Management & Computer Security—Un diario que trata sobre los últimos desarrollos en control de sistemas informáticos. MCB University Press Ltd., 60/62 Toller Lane, Bradford BD8 9BY, West Yorkshire, England; teléfono +44 (0) 1274 777700; fax +44 (0) 1274 785200; www.emeraldinsight.com/imcs.htm y feedback@emeraldinsight.com

Information Security Bulletin—Una revista que cubre una gran variedad de tópicos técnicos y gerenciales. Chi Publishing Ltd.; 26 Bunkers Hill, Lincoln LN2 4QP England; teléfono +44 (0) 1522-858280; fax +44 (0) 1522-858280; www.chi-publishing.com o isb@chi-publishing.com

Information Security Technical Report—Un diario que trata sobre detalles técnicos de cómo implementar productos de seguridad informática. Elsevier Science, 655 Avenue of the Americas, New York, NY 10010-5107 USA; teléfono (212) 633-3730; fax (212) 633-3680; www.elsevier.com y usinfo-f@elsevier.com

Information Security—Una revista que trata sobre todas las áreas del manejo de la seguridad informática. TruSecure, 1200 Walnut Bottom Road, Carlisle, PA 17013 USA; teléfono (888) 627-2281 or (717) 258-1816 ó (781) 255-0200; fax (781) 255-0215; www.trusecure.com/html/tspub/index.shtml o info@trusecure.com

Information Systems Auditor—Una revista que trata todos los aspectos de auditoría de sistemas informáticos de una manera concisa. International Newsletters, PO Box 133, Witney, Oxon OX8 6ZH Inglaterra; teléfono +44 (0) 1993 824130, fax +44 (0) 1993 824150; www.intnews.com; sales@intnews.com

Information Systems Security—Una revista que tiene que ver con consejos orientados a la gerencia sobre asuntos de seguridad informática. CRC Press, 2000 Corporate Blvd. NW, Boca Raton, FL 33431 USA; teléfono (800) 272-7737; fax (800) 374-3401; www.crcpress.com or orders@crcpress.com

Inside Fraud Bulletin—Un boletín informativo que trata con noticias y artículos de alta y baja tecnología. Maxima Partnering Limited, Hillend House, Nutley, East Sussex TN22 3HB, Inglaterra; teléfono +44 (0) 1825 712868 ó +44 (0) 1825 712069; fax +44 (0) 1825 712026; www.insidefraud.com; ifbulletin@maxima-group.com

Intelligence Online—Un boletín informativo que trata sobre información relacionada con espionaje industrial en seguridad informática. Indigo Publications Group, 142 rue Montmartre, F-75002 París, Francia; teléfono +33 1 44 88 26 10; fax +33 1 44 88 26 15; www.indigo-net.com and indigo@indigo-net.com

Information Systems Control Journal—Un diario de una asociación profesional que informa sobre auditorías EDP o de computación. Information Systems Audit and Control Association (ISACA), 135 South LaSalle, Dept. 1055, Chicago IL 60674-1055 USA; teléfono (847) 253-1545; fax (847) 253-1443; www.isaca.org/jrnldhome.htm

Journal of Computer Security—Un diario que trata sobre tópicos de investigación y desarrollo asociados con sistemas informáticos seguros. IOS Press, Nieuwe Hemweg 6B, 1013 BG Amsterdam, Holanda; teléfono +31 20 688 3355; fax +31 20 620 3419; www.iospress.nl y market@iospress.nl

Law Enforcement Product News—Una revista que trata sobre los nuevos productos y servicios para las autoridades policiales, seguridad física e industrias de prisiones e incluye cobertura de alguna información sobre productos de seguridad. General Communications, 100 Garfield St., Suite 300, Denver, CO 80206-5550 USA; teléfono (303) 322-6400; fax (303) 322-0627; www.law-enforcement.com

Managerial Auditing Journal—Un diario de cómo la actuación ampliada del auditor interno se está llevando a cabo, incluyendo formas para ayudar en vez de criticar a la gerencia. MCB University Press, Limited, 60/62 Toller Lane, Bradford BD8 9BY Inglaterra; teléfono +44 (0) 1274 777700; fax +44 (0) 1274 785200; www.mcb.co.uk/maj.htm; feedback@emeraldinsight.com

Manufacturing and Logistics IT—Un boletín informativo que trata sobre los últimos desarrollos en seguridad IT en todo el mundo, dándole especial énfasis a la seguridad para el comercio en Internet. IBC Ltd., Latimer House, 189 High Street, Potters Bar, Herts EN6 5DA Inglaterra; teléfono +44 (0) 1707 664200; fax +44 (0) 1707 664800; www.ibcpub.com

Operations Management—Un boletín informativo que trata de los aspectos legales y de seguridad asociados con la presencia en Internet. Institutional Investor Inc., 488 Madison Ave., New York, NY 10022 USA; teléfono (212) 224-3800; fax (212) 224-3689; www.operationsmanagement.com o customerservice@iinews.com

Password—Una revista para los especialistas en seguridad informática que trata de la certificación de profesionales, normas, políticas y asuntos relacionados. Information Systems Security Association (ISSA), 7044 S. 13th Street, Oak Creek, WI 53154 USA; teléfono (414) 768-8000, fax (414) 768-8001; www.issa-intl.org

Technical Security Branch—Un boletín informativo que trata de los asuntos de la gestión de seguridad informática. Technical Security Branch, Technical Operations Directorate, Royal Canadian Mounted Police, 1426 St. Joseph Blvd., Gloucester, Ontario, K1A OR2 Canada; teléfono (613) 993-8235; fax (613) 993-7060; www.rcmp-grc.gc.ca/tsb/pubs/index_e.htm; brian.feagan@rcmp-grc.gc.ca

Risk & Continuity—Un diario dirigido a la alta gerencia de grandes empresas, cubriendo todos los aspectos de planificación de contingencias incluyendo sistemas informáticos. Chi Publishing Ltd.; 26 Bunkers Hill, Lincoln LN2 4QP Inglaterra; teléfono +44 (0) 1522-858280; fax +44 (0) 1522-858280; www.chi-publishing.com o subs@chi-publishing.com

Risk Management Magazine—Una publicación dirigida a la gerencia sobre el manejo de los riesgos. Risk Management Society Publishing, Inc., 655 Third Ave., New York, NY 10017 USA; teléfono (212) 286-9292; fax (212) 922-0716; www.rims.org and www.rmmag.com

SC Magazine—Una revista que trata sobre los últimos desarrollos de productos y revisiones de los mismos. West Coast Publishing, 161 Winchester Road, Suite 201, Framingham, MA 01701 USA; teléfono (508) 879-9792; fax (508) 879-2755; www.scmagazine.com

Security Magazine—Una revista que trata de seguridad informática y con frecuencia artículos adicionales sobre seguridad informática. Business News Publishing, PO Box 941724, Plano, TX 95094 USA; teléfono (972) 509-0113; fax (972) 509-0764; www.securitymagazine.com

Security Insider Report—Un boletín informativo que trata sobre desarrollos de seguridad informática. A Infowar.com and Interpact, Inc., 3030 N. Rocky Drive

West #240, Tampa, FL 33607 USA; teléfono (813) 288-1955; fax (813) 288-1985; www.infowar.com/chezwinn/sir/sir_home.html-ssi

Security Law—Un boletín informativo que trata sobre casos judiciales, algunos de los cuales están relacionados con seguridad informática. Strafford Publications, 590 Dutch Valley Rd., NE, Atlanta, GA 30324-0729 USA; teléfono (404) 881-1141; fax (404) 881-0074; www.straffordpub.com

Security Management—Una revista que trata una gran variedad de tópicos de seguridad incluyendo coberturas especiales en seguridad informática. American Society for Industrial Security, 1625 Prince St., Alexandria, VA 22314-2818 USA; teléfono (703) 519-6200; fax (703) 519-6299; www.asisonline.org; asis@asisonline.com

Security Technology News—Un boletín informativo que trata sobre biometría, patentes y otros tópicos de protección de datos, además de una variedad de tópicos de seguridad física. BCC Publications, 25 Van Zant St., Norwalk, CT 06855-4266 USA; teléfono (203) 853-4266; fax (203) 853-0348; www.bccresearch.com

Security Watch—Un boletín informativo que cubre asuntos de seguridad física, pero incluye artículos sobre seguridad informática. Bureau of Business Practice, 125

Eugene O'Neill Drive, Suite 103, New London, CT 06320 USA; teléfono (800) 876-9105 ó (860) 442-4365 internacional; fax (800) 437-3150 gratuito; www.bbpnews.com; customer.service@aspenpubl.com

Telecom & Data Network Security—Un boletín informativo que trata sobre protección de centrales telefónicas privadas de fraude y abuso telefónico. Telecommunications Reports International, 1333 H St., NW, Suite 100 East, Washington, DC 20005-4707 USA; teléfono (800) 822-6338 ó (202) 312-6100; fax (202) 312-6065; www.tr.com/newsletters/tns/index.htm; customerservice@tr.com

Topical Issues on White Collar Crime—Trata sobre la naturaleza forense e investigativa de los delitos de computación. Association of Certified Fraud Examiners, The Gregor Building, 716 West Ave., Austin, Texas 78701 USA; teléfono (800) 245-3321 ó (512) 478-9070, fax (512) 478-9297; www.cfenet.com; info@cfenet.com

Apéndice C

LISTA DE ASOCIACIONES PROFESIONALES Y ORGANIZACIONES RELACIONADAS

GENÉRICAS

American National Standards Institute (ANSI), 25 West 43rd St., New York, NY 10036 USA. Tel. 212-642-4900 or 212-764-3274. Fax 212-398-0023. www.ansi.org. Una organización que redactó las normas en varios tópicos de seguridad informática, como el cifrado.

American Society for Industrial Security (ASIS), 1625 Prince St., Alexandria, VA 22314 USA. Tel. 703-519-6200. Fax 703-519-6299. www.asisonline.org. Una sociedad profesional orientada a la seguridad física, que frecuentemente se refiere a temas de seguridad informática en conferencias y publicaciones.

Association for Computing Machinery (ACM) Special Interest Group on Security, Auditability, and Control (SIGSAC), One Astor Plaza, 1515 Broadway, 17th floor, New York, NY 10036 USA. Tel. 800-342-6626 or 212-626-0500. Fax 212-944-1318. www.acm.org. Una asociación profesional que emite publicaciones y boletines informativos sobre seguridad informática.

Association of Contingency Planners (ACP), 7044 S. 13th Street, Oak Creek, WI 53154 USA. Tel. 414-768-8000 ext. 116. www.acp-international.com. La mas grande organización de planificación de contingencias dentro del área de seguridad informática..

Association of Information Technology Professionals, (AITP), 315 South Northwest Highway, Suite 200, Park Ridge, IL 60068-4278. Tel. 800-224-9371 u 847-825-8124. Fax 847-825-1693. www.aitp.org and tina_turnbull@aitp.org. Una asociación profesional orientada a la gerencia de computación, la cual celebra conferencias sobre el tema de seguridad y tiene un grupo especial que se dedica a temas de seguridad.

Association For Information Management Professionals, 4200 Somerset Dr., Suite 215, Prairie Village, KS 66208 USA. Tel. 800-422-2762 or 913-341-3808. Fax 913-341-3742. www.arma.org or hq@arma.org. Una organización que trata primordialmente sobre información impresa.

Computer Emergency Response Team (CERT), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890 USA. Tel. 412-268-7090. Fax 412-268-6989. www.cert.org o cert@cert.org. Una organización que supervisa las experiencias de pérdidas en Internet y prepara reportes especiales sobre vulnerabilidades.

Computer Professional for Social Responsibility (CPSR), P.O. Box 717, Palo Alto, CA 94302 USA. Tel. 650-322-3778. Fax 650-322-4748. www.cpsr.org. Una organización abocada a las infracciones de la privacidad, ética y temas relacionados con seguridad informática.

Computer Security Institute (CSI), 600 Harrison St., San Francisco, CA 94107 USA. Tel. 415-947-6320. Fax 415-947-6023. www.goci.com or csci@cmp.com. Una organización que celebra conferencias de seguridad informática, incluyendo una de las conferencias mas grandes del mundo sobre seguridad informática y mercadea una publicación técnica sobre seguridad informática, libros relacionados y un boletín mensual. .

Data Interchange Standards Association, Inc. (DISA), 333 John Carlyle St., Suite 600, Alexandria, VA 22314-5743 USA. Tel. 703-548-7005. Fax 703-548-5738. www.disa.org. Una organización que maneja temas de normalización de formateo de datos y de comunicación que incluye temas de seguridad.

Electronic Funds Transfer Association, 950 Herndon Parkway, Suite 390, Herndon, VA 20170 USA. Tel. 703-435-9800. Fax 703-435-7157. www.efta.org. Una organización que maneja temas de servicios financieros incluyendo la seguridad de los pagos electrónicos.

Electronic Industries Alliance, 2500 Wilson Blvd., Arlington, VA 22201-3834 USA. Tel. 703-907-7794. Fax 703-907-7501. www.eia.org. Una alianza de muchas compañías y asociaciones profesionales como Solid State And Semiconductor Technology Association, Government Electronics And Information Technology Association, y Consumer Electronics

Association, involucradas en el logro de apoyo político para la industria de computación en temas como la privacidad.

Electronic Messaging Association, The Open Group, 44 Montgomery St., Suite 960, San Francisco, CA 94104-4704 USA. Tel. 415-374-8280. Fax 415-374-8293. www.ema.org. Un consorcio para proveedores y neutral en tecnología que trabajó en normas para la seguridad en correo electrónico.

Electronic Privacy Information Center (EPIC), 1718 Connecticut Ave., NW, Suite 200, Washington, DC 20009 USA. Tel. 202-483-1140. Fax 202-483-1248. www.epic.org and info@epic.org. Una organización que publica un cierto número de reportes importantes sobre privacidad.

Federal Information Systems Security Educator's Association (FISSEA), Department of Commerce, National Institute of Standards and Technology, Bldg. 820, Rm. 426, Gaithersburg, MD 20899 USA. Tel. 301-975-3883. Fax 301-948-2067. csrc.nist.gov/organizations/fisseaa.html. Una organización que patrocina una conferencia anual y coordina actividades de seguridad informática para educadores en el gobierno.

Information Systems Audit & Control Association (ISACA), 135 South LaSalle, Dept. 1055, Chicago IL 60674-1055 USA. Tel. 847-253-1545. Fax 847-253-1443. www.isaca.org. La sociedad profesional más grande y antigua relacionada con seguridad informática que emite varias publicaciones sobre normas y una revista mensual.

Information Systems Security Association (ISSA), 7044 S. 13th Street, Oak Creek, WI 53154 USA. Tel. 414-768-8000. Fax 414-768-8001. www.issa.org. Una sociedad profesional orientada a practicantes de seguridad informática y que celebra conferencias anuales con Adiestramiento MIS y suministra un boletín informativo.

Institute of Electrical and Electronics Engineers (IEEE), 1828 L St., NW, Suite 1202, Washington, DC 20036-5104 USA. Tel. 202-785-0017. Fax 202-752-4929. www.ieee.org. Una organización que celebra conferencias de seguridad informática, participa en actividades sobre normas, emite un boletín sobre criptografía y publica libros relacionados con seguridad informática.

Institute of Internal Auditors (IIA), 249 Maitland Ave., Altamonte Springs, FL 32701-4201 USA. Tel. 407-830-7600. Fax 407-831-5171. www.theiia.org o iiat@theiia.org. Una organización que ofrece un punto de vista de auditoría financiera interna y tiene un grupo de interés especial que trata sobre seguridad informática.

International Federation for Information Processing (IFIP), Hofstraße 3, A-2361 Laxenburg, Austria; Tel. +43 2236 73616. Fax +43 2236 73616 9. www.ifip.or.at o ifip@ifip.or.at. Una organización que ofrece una variedad de conferencias técnicas sobre tópicos de computación incluyendo conferencias sobre seguridad informática.

International Information System Security Certification Consortium (ISC2), Oficina de Certificaciones office: PO Box 1117, Dunedin, FL 34697 USA. Tel. 888-333-4458 ó 727-738-8657. Fax 727-738-8522. Oficina de Operaciones: 860 Worcester Rd., Suite 101, Framingham, MA 01701 USA. Tel. 508-875-8400. Fax 508-875-8450. www.isc2.org. Una organización que administra las pruebas para las evaluaciones de los profesionales certificados en seguridad de sistemas de información (CISSP).

International Standards Organization (ISO), Bruselas, Bélgica, c/o American National Standards Institute (ANSI), 25 West 43rd St., New York, NY 10036 USA. Tel. 212-642-4900. Fax 212-398-0023. www.ansi.org o ansionline@ansi.org. Una organización que desarrolla normas internacionales en seguridad informática, principalmente ISO 17799, que trata sobre la gestión de la seguridad informática.

MIS Training Institute, 498 Concord St., Framingham, MA 01702-2357 USA. Tel. 508-879-7999. Fax 508-872-1153. www.misti.com. Una organización que realiza una variedad de conferencias de seguridad informática relacionadas con auditorías y seminarios de adiestramiento.

National Computer Security Center (NCSC), 9800 Savage Road, Fort Meade, MD 20755-6765 USA. Tel. 800-688-6115 ó 410-854-4371. Fax 410-854-4375. www.nsa.gov or radium.ansc.mil. Una agencia gubernamental asociada con el Departamento de Defensa que provee evaluaciones de productos de seguridad informática y lineamientos para la configuración de ciertos productos.

Security Industry Association, 635 Slaters Lane, Suite 110, Alexandria, VA 22314-1177 USA. Tel. 703-683-2075. Fax 703-683-2469. www.siaonline.org. Una asociación de fabricantes de equipos y otros vendedores en la industria de seguridad física que trata con temas de seguridad informática, desarrolla normas técnicas y se involucra en actividades políticas para obtener ciertos resultados legislativos.

Society of Competitive Intelligence Professionals, 1700 Diagonal Rd., Suite 600, Alexandria, VA 22314 USA. Tel. 703-739-0696. Fax 703-739-2524. www.scip.org e info@scip.org. Una organización que tiene que ver con la recolección ética de inteligencia competitiva y la prevención de espionaje industrial.

Software and Information Industry Association, 1090 Vermont Ave., 6th Floor, NW, Washington, DC 20005 USA. Tel. 202-289-7442. Fax 202-289-7097. www.siia.net. Una organización que aborda la privacidad y temas relacionados con la seguridad informática en sus estudios y testimonios del congreso.

The World Institute for Security Enhancement (WISE), PO Box 4646, Miami Lakes, FL 33014 USA. Tel. 305-825-0088. Fax 305-556-9639. www.worldinstitute.org y securitytraining@pobox.com. Una organización que proporciona educación e investigaciones interdisciplinarias en temas de seguridad, incluyendo seguridad informática.

POR INDUSTRIA

American Bankers Association, 1120 Connecticut Ave. NW, Washington, DC 20036 USA. Tel. 202-663-5000. Fax 202-663-7543. www.aba.com. Una organización que prepara y promulga normas específicas para la industria bancaria.

American Institute of Certified Public Accountants, 1211 Avenue of the Americas, New York, NY 10036 USA. Tel. 212-596-6200. Fax 212-596-6213. www.aicpa.org. Una organización que prepara lineamientos para los auditores que trabajan en asuntos de seguridad informática y publica una revista que trata temas de seguridad informática.

Bank Administration Institute, One North Franklin, Suite 1000, Chicago, IL 60606-3421 USA. Tel. 312-683-2464. Fax 312-683-2373. www.bai.org e info@bai.org. Una organización que publica un boletín que trata temas de seguridad informática.

Canadian Institute of Chartered Accountants, 277 Wellington Street West, Toronto ON M5V 3H2, Canada. Tel. 416-977-3222. Fax 416-977-8585. www.cica.ca. Una organización que ha desarrollado y publicado varias normas relacionadas con seguridad informática.

Information Technology Industry Council (ITIC), 1250 Eye St., NW, Suite 200, Washington, DC 20005 USA. Tel. 202-737-8888. Fax 202-638-4922. www.itic.org. Un consorcio de industrias de computación que están involucrados en el logro de apoyo político y en actividades de normas asociadas con seguridad informática.

International Association for Healthcare Security and Safety, P.O. Box 637, Lombard, IL 60148 USA. Tel. 888-353-0990 or 630-871-9936. Fax 630-871-9938. www.iahss.org or nancy@iahss.org. Una organización que trata temas de seguridad como la privacidad de un paciente y proporciona material educativo.

International Association of Financial Crimes Investigators, 385 Bel Marin Keys, Suite H, Novato, CA 94949 USA. Tel. 415-884-6600. Fax 415-884-6605. www.iafcii.org. Una asociación especialista en fraudes con tarjetas de crédito, que ahora maneja una amplia variedad de fraudes en transacciones financieras.

POR SEGMENTO DE MERCADO

Cisco, c/o Advanced Network Information, 3567 Benton St., Suite 248, Santa Clara, CA 95051 USA. Tel. 408-241-1314. Fax 707-371-4967. www.ani-training.com o www.cisco.com. Una organización que alberga varios grupos de usuarios para aquéllos involucrados en el área técnica de comunicación de datos, y suministra adiestramiento en seguridad informática, incluyendo certificaciones.

Computer Associates, World Headquarters, One Computer Associates Plaza, Islandia, NY 11749 USA. Tel. 631-342-6049. Fax 516-342-8179. www.cai.com. Una organización que alberga grupos de usuarios de paquetes de control de acceso a mainframes IBM.

International Biometric Association, 1444 I Street NW, Suite 700, Washington, DC 20005-6542 USA. Tel. 202-712-9049. Fax 202-216-9646. www.tibs.org o ibs@bostromdc.com. Una asociación de proveedores de equipos y sistemas biométricos.

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 USA. Tel. 425-882-8080. www.microsoft.com. Una organización que suministra grupos de usuarios para clientes, y certificaciones para profesionales en seguridad informática.

Redsiren Technologies, I4 Division (International Information Integrity Institute), 650 Smithfield St., Pittsburgh, PA 15222 USA. Tel. 253-952-0365. Fax 253-952-0365. www.i4online.com. Una organización que provee servicios de suscripción para organizaciones grandes y se dedica a los aspectos prácticos de la administración de seguridad informática.

SHARE (IBM users group), 401 N. Michigan Ave. Suite 2400, Chicago, IL 60611 USA. Tel. 888-574-2735 or 312-321-5160. Fax 312-644-6363. www.share.org. Una organización que ha preparado requerimientos de seguridad y publicado investigaciones en seguridad informática.

Apéndice D LISTA DE MÉTODOS SUGERIDOS PARA AUMENTAR NIVEL DE CONCIENCIA

Los siguientes tópicos no están organizados por prioridad, sino por el tipo de comunicación. Considere esta lista un menú del cual se pueden seleccionar las actividades adecuadas. No seleccione sólo uno o dos de los siguientes métodos, sino 10 ó 20 de ellos. La

repetición de las ideas en las políticas de seguridad informática es esencial. La repetición impresiona a los usuarios y otros públicos, porque sugiere la importancia que la gerencia brinda a la seguridad informática.

EN PERSONA

- Ofrezca cursos de adiestramiento anuales para los usuarios, los administradores de sistemas, los coordinadores de seguridad informática en sitios remotos, los nuevos empleados y el público identificado en los análisis de necesidades.
- Invite a oradores con experiencia en seguridad informática para que se dirijan al personal de toda la organización en reuniones de almuerzo, reuniones del personal del departamento y otras reuniones internas.
- Discuta ideas acerca de las políticas y otro material en las reuniones de orientación de nuevos empleados.
- Envíe a personal con influencia en sistemas informáticos a conferencias externas de seguridad informática.
- Realice videoconferencias en donde las personas de varios sitios discutan sobre seguridad informática.
- Efectúe simulacros de vulnerabilidad mediante ataques de penetración.
- Instale un computador especial de demostración y enseñe al personal mediante un modelo lo que pasa cuando un virus de expansión rápida ataca un computador personal.
- Conduzca evaluaciones de riesgos en seguridad informática, especialmente al hacer entrevistas y utilice otros métodos para comprometer al personal al proceso.
- Solicite al departamento Legal que realice un inventario de propiedad intelectual y una evaluación de riesgos pertinente.
- Obsequie pequeños premios tales como almuerzos gratis al personal ejemplar que observe las políticas y procedimientos.
- Emite advertencias que reflejen infracciones a las políticas.
- Efectúe auditorías internas de tecnología informática, verificando hasta dónde se cumplen.
- Contrate consultores externos para efectuar auditorías externas de tecnología informática con énfasis en el cumplimiento.
- Inicie un proceso de inventario de duplicación de software no autorizado donde se revisen los computadores personales para comprobar si tienen software ilegal.
- Instale un sistema de manejo de licencias de software con el cual verifica si todo el software en uso tiene licencia para ello y hable con las personas que tengan software no autorizado.
- Integre el adiestramiento de seguridad informática con otros materiales de adiestramiento en computación, como cursos para teletrabajadores, obligatorio antes de comenzar el trabajo a distancia.
- Exija que el personal tome exámenes en línea para comprobar que han leído la política de seguridad informática, y sólo si aprueban recibirán los privilegios del sistema que han solicitado.
- Requiera que el personal tome y apruebe un breve examen inmediatamente al entrar al sistema, antes de permitirles hacer cualquier otra cosa. Sea cuidadoso con implicaciones adversas a la productividad.

- Establezca y promueva la existencia de un comité gerencial de seguridad informática.
- Establezca un comité de administradores de sistemas además de personal de primera línea que deba ocuparse de seguridad informática.
- Invite a administradores de sistemas de diferentes sitios para almuerzos trimestrales para hablar sobre la seguridad.
- Comience a disciplinar personal por infracciones de las políticas de seguridad e informe a los demás sobre las razones de las medidas disciplinarias.
- Inicie la planificación estratégica, el desarrollo de nuevos productos y otras iniciativas que consideren la información y los sistemas informáticos como la llave de ventajas competitivas futuras.
- Prevenga el uso de servicios nuevos de sistemas, tal como el acceso a Internet, hasta que estén funcionando ciertos proyectos de seguridad, como un cortafuego.
- Evite que el nuevo software de aplicaciones de negocio entre en producción hasta que se instalen los controles adecuados. Hable con la gerencia sobre estos puntos.
- Establezca un nuevo proceso de aprobación de control de cambios, como la prohibición de establecer nuevas líneas telefónicas sin tener la aprobación del gerente de seguridad informática. Hable con el gerente sobre estos temas.
- Declare un día de amnistía para los infractores de seguridad informática que deseen obtener asistencia técnica o de otro tipo para poder cumplir a cabalidad.
- Pruebe los respaldos que los administradores departamentales de sistema lleven a cabo y discuta con los gerentes de departamentos si estos respaldos son adecuados.
- Adopte un día anual de Seguridad Informática en el cual se presenten materiales educacionales y eventos especiales. Coordine con el Día Nacional de Seguridad en Computación, si fuere posible.
- Inicie una investigación de alto perfil en falta de seguridad informática y comprometa a integrantes del personal en la investigación.
- Programe charlas con la alta gerencia para referirse a temas estratégicos con respecto a cambios en la cultura corporativa para apoyar la seguridad informática.
- Conduzca una encuesta dentro de la gerencia media y baja preguntándoles lo que piensan se debe hacer para mejorar la seguridad informática, de tal manera de ponerlos a pensar en algo en que quizás no piensen mucho.
- Realice una encuesta de clientes, proveedores y terceros preguntándoles sobre lo que piensan se debe hacer para mejorar la seguridad en las actividades de negocios computarizados.
- Conduzca un análisis de brecha mediante el cual se compare el adiestramiento existente de seguridad informática y los materiales de conciencia con el grupo de mensajes que la gerencia quiere comunicar; y prepare una propuesta gerencial para actualizar los materiales.

POR ESCRITO

- Añada preguntas sobre seguridad informática a las evaluaciones escritas sobre el desempeño. Un "Sí" o "No" sería suficiente en muchas organizaciones.
- Requiera la firma en una declaración de responsabilidad personal que indique que el empleado considera el cumplimiento de las políticas como condición para mantenerse empleado.
- Requiera la firma en un formato verificando que el empleado ha recibido copia, ha leído y entiende el manual de seguridad informática.
- Requiera que todos los empleados anualmente firmen una declaración diciendo que han leído y entendido el manual de Políticas de Seguridad Informática.
- Requiera a los usuarios que firmen una declaración de cumplimiento de la seguridad antes de obtener sus identificadores de usuario.
- Escriba artículos sobre seguridad para periódicos internos, boletines informativos y revistas.
- Emite periódicamente declaraciones escritas sobre políticas, procedimientos y normas técnicas.

- Emite panfletos o folletos para los usuarios finales describiendo un código de conducta.
- Publique un folleto de auto-enseñanza paso a paso sobre lo básico de la seguridad informática.
- Escriba memos atribuibles a la alta gerencia como recordatorio al personal sobre la seguridad.
- Distribuya copias de recortes importantes de periódicos y revistas técnicas.
- Coloque anuncios y señales en las oficinas para recordar a las personas acerca de la seguridad informática.
- Imprima rótulos y calcomanías y colóquelos en ubicaciones donde se vean, como en las copiadoras y las máquinas de fax.
- Haga rótulos especiales para discos, rieles de cintas y medios similares, indicando la confidencialidad, instrucciones de manejo y propiedad.
- Divulgue en las pizarras notas sobre seguridad.
- Coloque notas de seguridad en los sobres de pago y boletos de viaje.
- Integre ideas de seguridad con la documentación de procesos de desarrollo de sistemas.
- Emite memos de diseño de responsabilidades organizacionales en seguridad informática que clarifiquen áreas de responsabilidad confusas.
- Redacte descripciones ampliadas de puestos de trabajo para administradores de sistemas y otros, de manera que la seguridad informática esté incluida.
- Redacte declaraciones ampliadas de misión para varios departamentos de manera que la seguridad informática sea explícitamente reconocida como parte de sus estatutos.
- Prepare un documento de la arquitectura de la seguridad informática o integre la seguridad en los planes tecnológicos de la organización.
- Publique un manual de seguridad informática que contenga políticas, contactos y una lista de productos aprobados internamente.
- Elabore listas de verificación que informen cómo implantar una política de seguridad informática.
- Redacte instrucciones detalladas de respaldo e insista que el personal las cumpla.
- Desarrolle y pruebe un plan de contingencia que abarque las emergencias y desastres en los sistemas informáticos.
- Exija que los formularios de aceptación de riesgos en seguridad informática las firmen todos los gerentes a cargo de unidades que no cumplen y que no tengan intenciones de cumplir en el futuro cercano.
- Prepare acuerdos de confidencialidad y enseñe al personal cuándo deben ser utilizados.
- Prepare acuerdos de no competencia y enseñe al personal cuándo deben ser utilizados.
- Prepare avisos para distribuir a toda persona que tenga contacto con secretos industriales, notificándoles que determinada información es un secreto industrial y que debe ser manejada de acuerdo con políticas y reglas especiales.
- Prepare reportes sobre información reciente de incidentes de seguridad informática conjuntamente con recomendaciones para el mejoramiento de los controles, que se distribuyan sólo a personas que necesiten conocerlos.
- Prepare un resumen de leyes de seguridad informática y reglamentos importantes para la organización.

EN SISTEMAS

- Añada instrucciones de seguridad a programas de aplicaciones y pantallas de ayuda en los sistemas.

- Adquiera software de adiestramiento en computación que corra en computadores personales y que requieran que el personal lo revise. Esto debe reportar automáticamente en el computador personal del jefe de seguridad informática, cuántos trabajadores han completado su adiestramiento, con los sellos de hora y fecha, y firmas digitales para crear evidencia que puede ser admitida en un juicio, demostrando que el trabajador ha leído la política.
- Establezca exámenes en línea o preguntas que determinen lo bien que el personal entiende el material de información sobre seguridad informática, quizás entregando premios, o al menos la posibilidad de entrar en una rifa de premios, para aquellos que alcancen notas perfectas.
- Antes de otorgar a los usuarios acceso a ciertas aplicaciones o facilidades en el sistema, exíjales que asistan a un breve programa de adiestramiento en línea.
- Prepare un disco con software de seguridad para un computador personal que incluya rutinas de cifrado, una contraseña para el control de acceso, un disco de servicio de limpieza y un cuestionario de auto-evaluación.
- Utilice cuestionarios escritos o automatizados para medir el nivel de cumplimiento obtenido en una auto-evaluación.
- Utilice software especial de identificación de vulnerabilidades para verificar los parámetros de seguridad, alertando al personal de seguridad que existen problemas. Estos problemas pueden incluir sistemas operativos instalados incorrectamente y contraseñas que se pueden adivinar fácilmente.
- Instale software de detección de intrusos para monitorear los intentos de entradas a los sistemas internos y usar estos reportes como evidencia para justificar mayores inversiones.
- Establezca un servidor interno de Intranet y publique allí toda la información de seguridad informática.
- Coloque en Intranet una lista de las preguntas de mayor frecuencia, ofreciendo repuestas sobre seguridad informática, con la esperanza de reducir el tiempo que el personal del departamento de Seguridad informática utiliza en contestar estas preguntas.
- Establezca mecanismos de búsqueda de palabras claves en el servidor de Intranet del departamento de Seguridad Informática, de tal manera que las personas puedan rápidamente ubicar el material de interés.
- Establezca filtros por cargo para la documentación de seguridad informática e integre estos filtros a la Intranet permitiendo a las personas ver solamente la documentación que ellos necesitan de acuerdo a su puesto de trabajo.
- Establezca software para bloquear acceso a sitios web a nivel del cortafuego para controlar los sitios que el personal visita y emitir un memo explicando el nuevo sistema.
- Instale software para monitorear el contenido del material que pasa a través del cortafuego, e informe al personal que su comunicación está siendo monitoreada.
- Exija que todos los computadores personales portátiles utilizados para realizar los negocios de la Empresa X tengan un paquete de software con un control de acceso que incluya una contraseña de inicio y un blanqueador de pantalla.
- Adopte un producto comercial de cifrado como una norma interna y publique las formas en que esto ayuda a la organización, dando un paso hacia la implantación de una infraestructura de clave pública.
- Establezca sistemas de registros que detecten infracciones de seguridad, y elabore un proceso formal para notificar a los usuarios y sus gerentes.
- Cambie el mensaje de bienvenida para evitar las transgresiones electrónicas, y declare que las facilidades del sistema son sólo para los negocios y que toda actividad de otro tipo será monitoreada.
- Coloque una nota en la pantalla de inicio, en el cortafuego o en los servidores de acceso remoto, informando a los usuarios que no deben continuar a menos que hayan revisado y entendido la política de seguridad informática.
- Establezca una pantalla que aparece después que el usuario se conecte y que cambie cada vez que se conecte, la cual resuma la política de seguridad informática, y que requiera que el usuario haga un clic en OK antes de seguir adelante.

- Exija al usuario hacer clic en un botón al momento de conectarse a las redes o sistemas informáticos de la Empresa X, indicando su aceptación de cumplir todas las políticas de seguridad informática.
 - Cambie los titulares para aplicaciones específicas, incluyendo correo electrónico, para proporcionar políticas de seguridad específicas de ciertas aplicaciones u otras instrucciones de seguridad.
 - Instale recordatorios cambiantes en las pantallas, similares a los que aparecen al inicio de sesión.
 - Utilice agentes de software que recuerden al personal efectuar ciertas actividades de seguridad, como el hacer copias de respaldo de sus sistemas con regularidad.
 - Proporcione a los administradores de sistemas la dirección de correo electrónico del Equipo de Repuesta ante Emergencias de Computación y hágales llegar la información sobre vulnerabilidades.
-
-

POR OTRAS VÍAS

- Escriba mensajes de seguridad informática en tazas de café, en la almohadilla del mouse, en vasos, abridores de sobres y cualquier objeto que reciba el personal.
- Resuma mensajes de seguridad en bloques de notas que se suministre gratuitamente al personal.
- Escriba mensajes de seguridad en camisetas y sudaderas y entréguelas al personal que respalda los esfuerzos de seguridad informática.
- Prepare cintas de video para su distribución en todas las instalaciones remotas, a menudo montando material de videos anteriores.
- Establezca una línea caliente con una máquina contestadora donde se puedan reportar problemas de seguridad informática de manera anónima.
- Circule materiales de concientización en cubículos o cabinas que contengan computadores personales, o en circuitos cerrados de televisión en áreas solamente para el personal, como el comedor.
- Transmite mensajes en la estación de televisión interna de la organización.
- Escriba mensajes de seguridad en los ambientadores que el personal coloca en el espejo retrovisor de su vehículo.



Apéndice E

ARMONIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD CON INTERFACES EXTERNAS DE RED

Muchos especialistas en sistemas informáticos se sienten confundidos cuando la gerencia les da instrucciones de conectar la red interna de su organización con la red interna de otra organización. Esta otra organización puede ser un proveedor, un cliente mayor, un subcontractista, una agencia del gobierno o una organización de contratación externa. Estas conexiones pueden, por ejemplo, establecerse a través de una extranet, de una red electrónica de intercambio de datos de terceros o de una web intermediaria de negocio a negocio.

Quien quiera que sea el tercero, y cualquiera que sea la naturaleza del arreglo del negocio, es vital que los participantes en esta nueva red estén de acuerdo en ciertas políticas fundamentales de seguridad. Si estas políticas de seguridad son incompatibles, entonces la falta de seguridad adecuada en una organización puede inducir a incidentes de seguridad en la otra organización. Por ejemplo, supongamos que una organización utilizó identificadores de usuarios por grupos y tuvo un serio argumento con un trabajador en particular, quedando éste descontento. Este trabajador podría alterar la red, pero los registros del sistema no podrán señalar exactamente quien está causando el problema. Debido a la conexión que se permitió establecer con la organización externa, los sistemas conectados a la red de dicha organización pueden ser dañados por ese trabajador descontento.

Para ayudar en la armonización de las políticas de seguridad de organizaciones que buscan establecer conexiones de redes, este capítulo proporciona una lista

de puntos esenciales de política. Estos puntos pueden ser utilizados por la gerencia en el momento de negociar el convenio. Si eso no ocurre, pueden al menos ser utilizados por el personal técnico al momento de llevar a cabo el convenio negociado. En algunos casos, una revisión de esta lista indicará que el convenio debe ser renegociado antes de aplicar los sistemas que reflejan dicho convenio.

La intención de armonizar las políticas de seguridad es la de establecer una base o norma de debido cuidado que todas las partes de un acuerdo deben seguir. Esta base debe definir los requerimientos mínimos de seguridad informática que se deben mantener para participar en el trabajo en red. El no desechar o no ser capaz de cumplir estos requerimientos debe ser razón suficiente para justificar la exclusión o expulsión del convenio multiorganizacional de trabajos en red.

Las áreas del tópico de seguridad informática abajo señaladas, están acompañadas por el número de sección correspondiente en esta publicación *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*, donde se encontrarán detalles sobre el tópico. La siguiente lista supone que la conexión a la organización externa se logra a través de Internet. Si la conexión es a través de discado, referirse al punto “[9.04.03 Autentificación del Usuario para Conexiones Externas](#)” en la página 344.

CONSIDERACIONES EN CONTROL DE ACCESO

Identificadores de usuario que reflejan usuarios individuales en vez de grupos de personas, ver “[9.02.01 Registro de Usuarios](#)” en la página 313.

Longitud de las contraseñas fijas empleadas y reglas de construcción, ver “[9.05.04 Sistema de Manejo de Contraseñas](#)” en la página 357.

Cambios en la contraseña una vez pasado cierto tiempo, ver “[9.05.04 Sistema de Manejo de Contraseñas](#)” en la página 357.

Cambios de contraseñas en las nuevas asignaciones o reposición de las contraseñas, ver “[9.02.03 Gestión de Contraseñas de Usuario](#)” en la página 324.

Sistemas de autenticación extendida del usuario como la contraseña de un solo uso, ver “[9.04.03 Autenticación del Usuario para Conexiones Externas](#)” en la página 344.

Cookies para autenticar el uso específico de un computador para conectarse, ver “[9.05.04 Sistema de Manejo de Contraseñas](#)” en la página 357.

Cookies cifradas o protegidas con firmas digitales para evitar engaños, ver “[9.05.04 Sistema de Manejo de Contraseñas](#)” en la página 357.

Prevención del anonimato del usuario a través del proceso de inicio de sesión, ver “[9.02.01 Registro de Usuarios](#)” en la página 313.

Asignación de privilegios a usuarios basados en la necesidad de conocer, ver “[9.02.02 Administración de Privilegios](#)” en la página 320.

Remoción de los privilegios de acceso tan pronto un trabajador autorizado se retira, ver “[9.02.01 Registro de Usuarios](#)” en la página 313.

Revocación de privilegios a los usuarios que no utilizan sus identificadores, ver “[9.02.01 Registro de Usuarios](#)” en la página 313.

Finalización de la sesión después de un período sin actividad, ver “[9.05.07 Desconexión por Tiempo](#)” en la página 370.

Utilización de sistemas de inicio individual u otras puertas de entradas para usuarios, ver “[9.05.03 Identificación y Autenticación del Usuario](#)” en la página 354.

Tipos de cortafuego, enrutadores y otros sistemas de control de flujo, ver “[8.05.01 Controles de las Redes](#)” en la página 203.

Uso de zonas desmilitarizadas como filtro para atacantes, ver “[8.05.01 Controles de las Redes](#)” en la página 203.

CONSIDERACIONES EN CIFRADO Y EN INFRAESTRUCTURA DE CLAVE PÚBLICA

Proceso de cifrado utilizado para transmisiones de datos confidenciales, ver “[8.06.03 Procedimientos para el Manejo de la Información](#)” en la página 223.

Proceso de gestión de claves de cifrado utilizado para manejar automáticamente las claves, ver “[10.03.05 Manejo de Claves](#)” en la página 415.

Utilización de hardware y software para el suministro de cifrado, ver “[10.03.02 Cifrado](#)” en la página 410.

Certificados digitales como mecanismo para identificar usuarios, ver “[10.03.03 Firmas Digitales](#)” en la página 414.

Certificados digitales para restringir los privilegios de usuarios específicos, ver “[10.03.03 Firmas Digitales](#)” en la página 414.

Verificación de antecedentes para la emisión de certificados digitales, ver “[10.03.03 Firmas Digitales](#)” en la página 414.

Certificación cruzada de autoridades certificadoras para apoyar los certificados digitales, ver, “[10.03.05 Manejo de Claves](#)” en la página 415.

Listas de revocación de certificados y otros procedimientos para inhabilitar usuarios, ver “[10.03.05 Manejo de Claves](#)” en la página 415.

Billeteras electrónicas para proteger certificados digitales y otras informaciones, ver “[10.03.05 Manejo de Claves](#)” en la página 415.

Firmas digitales para garantizar ausencia de cambios a ciertos datos, ver “[10.03.05 Manejo de Claves](#)” en la página 415.

Firmas digitales para garantizar que los datos se originaron con ciertas personas, ver “[10.03.05 Manejo de Claves](#)” en la página 415.

CONSIDERACIONES EN CONTROL DE CAMBIOS Y PLANIFICACIÓN DE CONTINGENCIAS

Software y procedimientos para detección y erradicación de virus, ver “[8.03.01 Controles Contra Software Malicioso](#)” en la página 186.

Proceso de autorización de control de cambios para todos las modificaciones hechas a la red, ver “[10.05.01 Procedimientos para el Control de Cambios](#)” en la página 427.

Instalación rápida de los parches suministrados por vendedores de cortafuegos y sistemas operativos, ver “[10.05.02 Revisión Técnica de los Cambios en Sistemas Operativos](#)” en la página 434.

Pruebas del software nuevo previa utilización en ambientes de redes de producción, ver “[10.04.01 Control del Software de Operaciones](#)” en la página 425.

Movilización por ataques, del equipo de respuesta ante emergencias computacionales, ver “[8.01.03 Procedimientos de Gestión de Incidentes](#)” en la página 173.

Plan de contingencia para lidiar con desastres y otros eventos importantes, ver “[11.01.03 Redacción e Implementación de Planes de Contingencia](#)” en la página 440.

Sistema de detección de intrusos notifica a los técnicos acerca de la intrusión, ver “[8.05.01 Controles de las Redes](#)” en la página 203.

Medidas de seguridad física para todos los centros de datos conectados a la red, ver “[7.01.03 Aseguramiento de Oficinas, Salones e Instalaciones](#)” en la página 148.

Sistemas de electricidad sin interrupciones para prevenir el tiempo de inactividad por fallas eléctricas, ver “[7.02.02 Suministro Eléctrico](#)” en la página 158.

CONSIDERACIONES EN GESTIÓN DE REDES

Observación por parte de la gerencia de la información enviada a través de la red - privacidad, ver “[12.01.04 Protección de los Datos y Privacidad de la Información Personal](#)” en la página 457.

Sellos de hora y fecha para validar que cierta actividad ocurrió, ver “[9.07.01 Registro de Eventos](#)” en la página 378.

Fuentes y procedimientos de la sincronización del tiempo en la red, ver “[9.07.03 Sincronización del Reloj](#)” en la página 389.

Registros y pistas de auditoría grabados en máquinas de los clientes y servidores, ver “[9.07.01 Registro de Eventos](#)” en la página 378.

Sistema de gestión de redes y visibilidad de máquinas específicas, ver “[8.05.01 Controles de las Redes](#)” en la página 203.



Apéndice F

LISTA DE VERIFICACIÓN DE PASOS EN PROCESO DE DESARROLLO DE POLÍTICAS

Esta lista de verificación está dirigida a suministrar una visión general de los pasos principales relacionados con el desarrollo, mejoramiento y aprobación de un documento interno de políticas de seguridad informática. Para una descripción más detallada de los pasos necesarios para el desarrollo, mejoramiento y aprobación ver Capítulo 2, “[Instrucciones](#).” Para una lista de pasos para complementar una política, después de que ésta se ha generado, ver Apéndice I, “[Sugerencias para los Próximos Pasos](#).” Muchos de los pasos siguientes se pueden lograr de manera simultánea o en un orden diferente al que sigue:

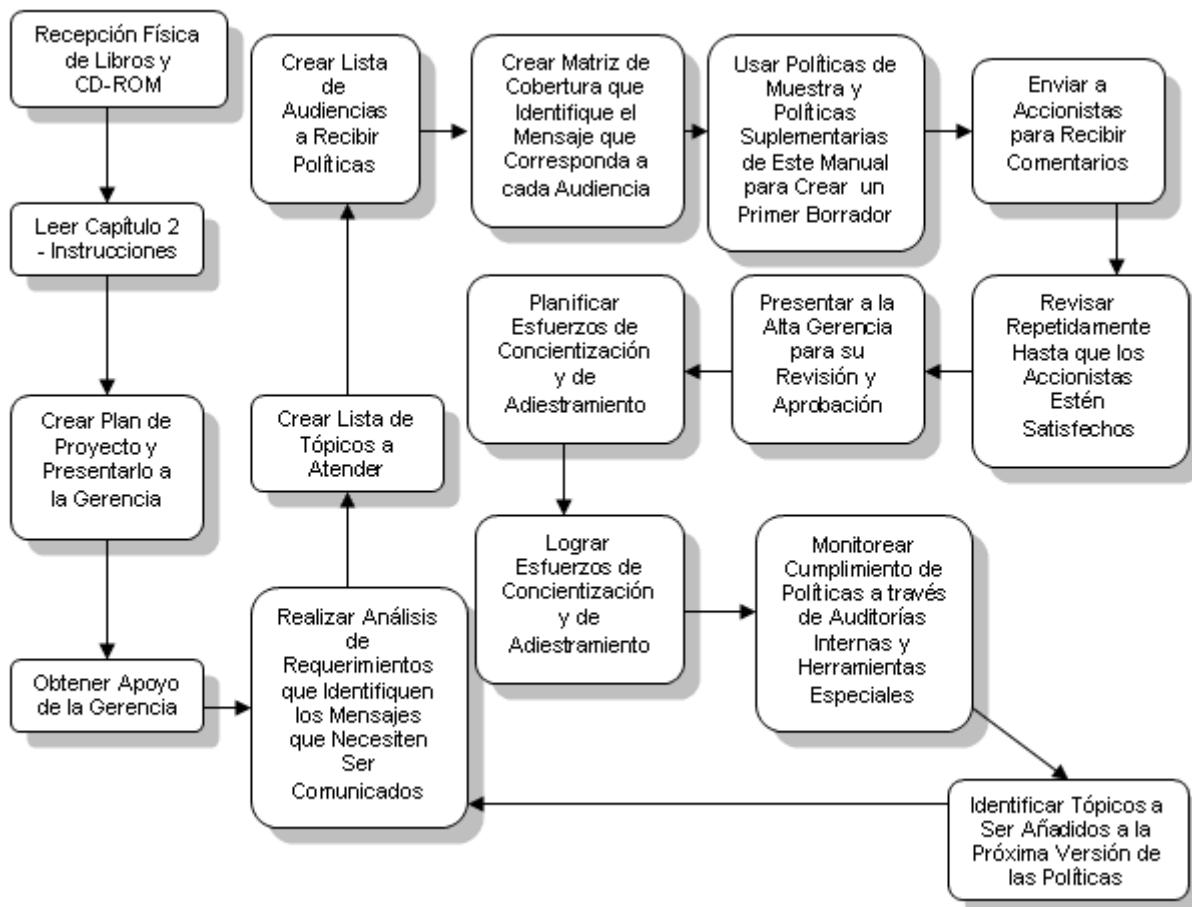
- 1 Realizar una evaluación de riesgo o una auditoría de tecnología informática para determinar las necesidades particulares de seguridad informática de la empresa. Estas necesidades deben estar explícitas en un documento de políticas.
- 2 Especificar lo que significa la palabra “política” dentro de la organización, de tal manera que no se esté elaborando un “procedimiento”, una “norma” u otro material.
- 3 Garantizar que los roles y responsabilidades relacionados con la seguridad informática están claros, incluyendo la responsabilidad de emitir y mantener políticas.
- 4 Convencer a la gerencia que es aconsejable tener políticas de seguridad informática documentadas.
- 5 Identificar al personal de la alta gerencia y a los críticos que aprobarán el documento final de seguridad informática.
- 6 Recolectar y leer toda la información interna sobre el material que crea conciencia en cuanto a la seguridad y elaborar una lista de los mensajes que se encuentran en el pie de página.
- 7 Llevar a cabo una breve encuesta interna para recolectar ideas que los participantes piensen deben estar incluidas en una política de seguridad informática nueva o actualizada.
- 8 Examinar otras políticas emitidas por su organización tales como las emitidas por la gerencia de Recursos Humanos, para identificar el formato predominante, el estilo, el tono, la longitud, y las referencias cruzadas. El objetivo es generar una información que esté acorde con esfuerzos previos.
- 9 Identificar la audiencia que va a recibir la información sobre seguridad informática y determinar si cada una va a recibir un documento por separado o una página aparte en un sitio Intranet.
- 10 Determinar hasta qué punto dicha audiencia tiene conocimientos informáticos, y cuán receptiva es a mensajes sobre seguridad. Esto incluye el entender la cultura corporativa sobre seguridad informática.
- 11 Decidir si se deben llevar a cabo esfuerzos adicionales para crear conciencia antes de que se emitan las políticas de seguridad informática. Por ejemplo, un esfuerzo puede mostrar que la información por sí misma se ha convertido en un factor crítico de producción.
- 12 Utilizar ideas del ejercicio de evaluación de riesgo, preparar una lista de mensajes absolutamente necesarios sobre la política que se deban comunicar. Consultar los estatutos sobre la política así como los modelos de las políticas que se encuentran en este manual.
- 13 Si existe más de un tipo de audiencia, hay que comparar dichas audiencias con los mensajes elementales a comunicar a través de la matriz de cobertura. Para mayor información, ver Capítulo 2, “[Instrucciones](#).”
- 14 Determinar cómo se difundirá el material de la política, haciendo énfasis en las limitaciones e implicaciones de cada medio de comunicación. Se recomienda un sitio de intranet, pero el apéndice que maneja los métodos de creación de conciencia proporciona muchas alternativas.

- 15 Revisar el proceso de verificación del cumplimiento y el proceso disciplinario, para garantizar que todos puedan trabajar sin obstáculos con el nuevo documento de políticas.
- 16 Determinar si el número de mensajes es muy grande para que se manejen al mismo tiempo, y de ser así, identificar categorías diferentes de material que se emitirán eventualmente.
- 17 Tener un esquema de los tópicos a incluir en el primer documento revisado por varios participantes. Un comité gerencial de seguridad informática constituye la comisión ideal de revisión.
- 18 Basados en comentarios de los actuantes, revisar el esquema original y preparar un primer borrador, extrayendo de este manual las políticas conforme se vayan necesitando.
- 19 Tener el primer borrador revisado por los actuantes para las primeras reacciones, sugerencias sobre la presentación e ideas para la puesta en práctica.
- 20 Revisar el borrador en respuesta a los comentarios de los actuantes. Estar a la expectativa de que este paso se repetirá varias veces.
- 21 Solicitar la autorización de la política por la alta gerencia. Puede que hagan falta cambios, en cuyo caso este paso se repetirá varias veces.
- 22 Preparar extractos del documento de política para ciertos objetivos. Por ejemplo, para un formato firmado por los usuarios que reciban identificadores de usuario y contraseñas nuevas o renovadas.
- 23 Preparar un plan de creación de conciencia que utilice la política como una fuente de ideas y de requisitos.
- 24 Generar un memorando sobre los papeles de trabajo, indicando lo que se hizo con los comentarios recibidos de los críticos, aun cuando no se hayan realizado cambios.
- 25 Escribir un memorando acerca del proyecto, el aprendizaje obtenido, lo que amerita cambio para que la nueva versión del documento de políticas se prepare con mayor eficiencia y con mayor receptividad por parte de los lectores, y que responda mejor a las circunstancias únicas que enfrenta la organización.
- 26 Preparar una lista con los próximos pasos que serán requeridos para poner en práctica los requisitos especificados en el documento de políticas. Esto puede incluir el desarrollo de una arquitectura de seguridad informática, documentos de procedimientos manuales y normas técnicas de seguridad informática, la adquisición de productos nuevos, la contratación de personal técnico nuevo y otros asuntos.



Apéndice G VISTA GENERAL DE LAS TAREAS DEL PROCESO DE DESARROLLO DE LAS POLÍTICAS

Figura G-1: Vista General del Proceso de Desarrollo de las Políticas





Apéndice H PROBLEMAS REALES OCASIONADOS POR LA AUSENCIA DE POLÍTICAS

AGENCIA GUBERNAMENTAL

Un oficinista invertía buena parte de su tiempo laboral navegando en Internet. Debido a que no existía una política que especificara lo que constituía uso personal excesivo, la gerencia no podía disciplinar a este empleado. Entonces, la gerencia descubrió que el oficinista había descargado una gran cantidad de material pornográfico. Utilizando esto como justificativo, la gerencia lo despidió. El oficinista presentó una apelación a esta rescisión de la relación laboral ante la

Comisión de Funcionarios del Estado, alegando que no podía ser despedido debido a que no se le había notificado la prohibición de descarga de pornografía. Después de una audiencia, la comisión ordenó que se le reintegrara a su antiguo puesto con pago de todos los salarios caídos. Esta situación se pudo haber evitado si el patrono hubiera tenido una política clara y vigente que manejara el uso personal de los sistemas de información.

BUFETE DE ABOGADOS

El gerente de procesamiento de datos aceptó un trabajo en un bufete de abogados de la competencia. Debido a que su patrono anterior no contaba con nadie que realizara su trabajo, lo mantuvieron como contratista a medio tiempo. Por muchos meses, este técnico altamente especializado desempeñó una amplia variedad de tareas de administración de sistemas para su primer patrono. Para poder realizar estas tareas, necesitaba todos los privilegios en la red de su primer patrono. Un día, un socio del primer patrono se enteró que el nuevo patrono del gerente había decidido hacer de contraparte en una demanda muy publicitada que llevaban. Los

socios del primer patrono del gerente comenzaron a realizar preguntas, tales como si el gerente anterior de procesamiento de datos podía acceder a cualquier archivo dentro de la red y posiblemente a las estrategias legales de este caso. La respuesta fue afirmativa, pero nadie supo si el gerente había aprovechado estas facilidades debido a que no se mantenían registros de acceso a los datos. Esta situación se habría podido evitar si el patrono anterior hubiese mantenido políticas bastante sencillas sobre conflictos de intereses, privilegios de acceso a los sistemas, y si hubiese mantenido los registros correspondientes.

EMPRESA PETROLERA

Un técnico en computación de una empresa petrolera recopiló una lista de chistes sobre sexo. Orgulloso de su lista, la transmitió a través de Internet, anexó su dirección de correo electrónico al final, en caso de que los receptores tuvieran chistes nuevos. La gerencia logró eliminar la lista de varios grupos de discusión, pero no pudo controlar las copias que ya habían sido elaboradas. Al mismo tiempo este técnico imprimió una copia de esta lista, se distrajo y la dejó en la impresora. Las

damas del departamento formularon quejas por la exposición a chistes sobre sexo a través del correo electrónico, que no les gustaban. Ellas mostraron las publicaciones en Internet y las copias impresas como pruebas. La demanda pendiente por acoso sexual se arregló con una suma no divulgada. Era evidente la falta de una política acerca el uso permitido a través de Internet, y de una política sobre las ofertas realizadas a nombre de la empresa en Internet.

PERIÓDICO LOCAL

Un periódico local no disponía de una política acerca de la vigencia de un identificador de usuario y de los privilegios de las contraseñas después de que un

empleado abandonara la empresa. Un reportero abandonó el periódico, y poco después, el periódico afrontó problemas debido a que un periódico local de la

competencia en forma consistente tomaba sus historias exclusivas sobre investigaciones. Una revisión de los registros de los sistemas reveló que el reportero que había abandonado el trabajo, se había estado conectando constantemente con el computador de su patrono

anterior para obtener ideas para sus historias con su patrono actual. Este acceso se pudo haber evitado si el periódico hubiera adoptado una política que eliminara los privilegios de acceso de los trabajadores despedidos.

EMPRESA MANUFACTURERA DEL MEDIO OESTE NORTEAMERICANO

Un chiste sobre un virus enviado por correo electrónico a través de Internet alertó a la gente que si recibía un mensaje con el encabezado “Únete a la Tripulación” no debían leerlo. El chiste continuaba diciendo que, de ser desplegado, el correo electrónico borraría el disco duro. Pensando que estaban haciendo un favor a los demás, 10% del personal de una gran empresa manufacturera transmitió el chiste a toda la gente que conocían. Debido

a que ninguna política definía cómo manejar estas advertencias, inundaron las redes internas de la empresa con correos electrónicos y generaron una gran pérdida de tiempo al personal técnico. Una política que exija que toda la información registrada sobre vulnerabilidades en la seguridad sea enviada al departamento de Seguridad Informática, habría evitado esta pérdida de tiempo de los trabajadores.

EMPRESA MANUFACTURERA DE LA COSTA OESTE NORTEAMERICANA

Debido a que no disponía de una política que solicitara que los datos confidenciales de los empleados estuvieran cifrados mientras estuvieran almacenados, una empresa grande de manufacturas enfrentó un problema de relaciones públicas. Un ladrón hizo un gran negocio al extraer un disco de un computador con detalles personales e información sobre cuentas

bancarias de más de 20.000 empleados y ex-empleados. La prensa especuló que esto se podría utilizar para el robo de identidades, incluyendo la solicitud de tarjetas de crédito a nombre de otras personas. El evento precipitó un proceso de notificación masiva, inclusive recomendaciones sobre cambios en los números de cuentas bancarias.

EMPRESA IMPORTANTE DE SERVICIOS EN LÍNEA

Un hombre enlistado en la Armada se registró con una empresa en Internet de servicios en línea y llenó un formato en el cual aclaraba que era homosexual. Un empleado de la empresa de servicios, después de una solicitud por parte de la Armada, compartió esta información del perfil del candidato con representantes de “alto rango” de la Armada. Basada en esta información, la Armada dio de baja al hombre en forma deshonrosa. El hombre luego la demandó por violar su propia política, y logró una baja honorable con benefi-

cios de jubilación. La empresa de servicios en línea declaró públicamente que su empleado había violado la “política de privacidad”, pero la política había sido violada en varias ocasiones anteriores, incluyendo la muy publicitada intención de la alta gerencia de vender los números telefónicos de sus clientes a proveedores de telemarketing. Por lo menos la organización de servicios admite ahora que cuenta con una política. El adiestramiento asociado con políticas es absolutamente esencial si estas políticas van a ser acatadas fielmente.



Apéndice I SUGERENCIAS PARA LOS PRÓXIMOS PASOS

Existen muchos caminos disponibles después de la aprobación de una política de seguridad informática. La siguiente lista de próximos pasos sugeridos brinda algunas respuestas, pero no está dirigida a proporcionar una lista completa de todos los próximos pasos. Cada uno de estos próximos pasos sugeridos son comunes, aunque no siempre se aplicarán a todas las organizaciones. Se deberían utilizar como un punto de partida cuando se genera un plan para poner en práctica las políticas de seguridad informática. Las sugerencias están organizadas en un orden cronológico aproximado, y se pueden revisar de manera individual, aunque una mejor alternativa sería lograr varios de estos pasos al mismo tiempo, con el objetivo de avanzar con rapidez.

Es posible que existan varios proyectos iniciados como resultado de la conformación de una política de seguridad informática. Por ejemplo, el esfuerzo de preparación de una política pudo haber resaltado el hecho de que un requisito actual de seguridad informática es obsoleto. Un ejemplo específico incluye una tecnología de devolución de llamadas para acceder a las redes de la empresa. Si este requisito está ampliamente respaldado dentro de la organización, el esfuerzo para adoptar una alternativa más actualizada puede resultar en otro proyecto que será anexado al proyecto principal. Continuando con este ejemplo específico, se podrían utilizar las tarjetas de contraseñas dinámicas, en vez de los sistemas de devolución de llamadas.

Publicar Políticas en Intranet o Equivalente—El documento nuevo debería ser colocado en la Intranet de la Empresa X, y se deberían añadir enlaces a los documentos asociados. Se deberían preparar múltiples índices para que los usuarios ubiquen rápidamente el material de interés. Se debería añadir una palabra clave como herramienta de búsqueda. El documento podría estar incluido en otros medios equivalentes a los foros electrónicos, por ejemplo un kiosko de Recursos Humanos. Para mayor información sobre dónde colocar las políticas, ver Apéndice D, “[Lista de Métodos Sugeridos para Aumentar Nivel de Conciencia](#).”

Desarrollar un Cuestionario de Autoevaluación—Los requisitos esenciales en el nuevo documento de políticas de seguridad informática se deberían extraer y reformular en la forma de un cuestionario. Auditoría Interna debería emitir el cuestionario a los gerentes departamentales. Las respuestas a los cuestionarios resaltarán las áreas en las cuales los departamentos no

están dentro de los parámetros y donde se necesitan mejoras adicionales en los controles. De acuerdo con los resultados de las encuestas, se pueden proponer proyectos de mejora. El cuestionario puede ser parte de un proceso de auditoría interno de chequeo de cumplimiento. Para mayor información en el logro del cumplimiento, ver “[Manejo del Incumplimiento](#)” en la página 34.

Desarrollar Formulario Revisado de Emisión de Identificador de Usuario—Un formato se utiliza en muchas organizaciones como una forma de documentar la autorización de la gerencia previo a la emisión de un identificador de usuario. Para mayor información acerca de este tópico, ver “[Formularios para Identificadores de Usuario](#)” en la página 318. Se debería incluir un resumen de las ideas críticas plasmadas en el nuevo documento de políticas de seguridad informática como parte de este formulario, conjuntamente con palabras tales como “el usuario abajo mencionado ha leído y está de acuerdo en seguir las políticas de la empresa X como condición para usar los sistemas de información de dicha empresa”. Todo identificador de usuario nuevo o renovado sólo se puede activar si el formulario se ha completado.

Desarrollar Formulario de Convenio de Cumplimiento de Políticas de Seguridad Informática—Un documento legal que refleje un acuerdo por parte de los empleados de cumplir con las políticas de seguridad informática debe ser elaborado, editado, y posteriormente autorizado por la gerencia. Este formato debe estar firmado por todos los trabajadores, o por lo menos por todos los trabajadores empleados recientemente o los que se haya retenido. Se debería iniciar un programa de creación de conciencia para publicitar la existencia de la nueva política y obtener formularios firmados. Para un ejemplo de este acuerdo y mayor información en cuanto al cumplimiento de las políticas, ver Apéndice J, “[Convenio de Cumplimiento de las Políticas de Seguridad Informática](#).”

Desarrollar Pruebas para Determinar si los Trabajadores Entienden las Políticas—Se puede desarrollar un conjunto de pruebas para verificar si los trabajadores entienden los puntos esenciales de un documento de políticas de seguridad informática. Las pruebas se pueden utilizar para obtener ciertos privilegios. Por ejemplo, sólo si el trabajador pasa un examen, se

activarán los privilegios de para trabajo remoto. Para mayor información acerca de este tópico, ver “[Exámenes Sobre las Políticas](#)” en la página 117.

Asignar Coordinadores de Seguridad Informática

—Muchos departamentos centralizados de Seguridad Informática cuentan con poco personal y no pueden manejar todos los trabajos de seguridad informática que se deben llevar a cabo. Para ayudar en la puesta en práctica de los controles descritos en la nueva política, se deben asignar coordinadores descentralizados de seguridad informática. Los administradores de sistemas, los gerentes de sistemas, los administradores de redes y demás personal técnico pueden apoyar esta actividad a medio tiempo. Los coordinadores sirven de enlace con el grupo de seguridad informática central, al interpretar las políticas para un departamento o división. Para mayor información en cuanto al rol de un coordinador de seguridad informática, ver “[Enlaces de Seguridad Informática](#)” en la página 47.

Adiestrar Coordinadores de Seguridad Informática

—Antes de que los coordinadores de seguridad informática puedan realizar un trabajo substancial, deben recibir el adiestramiento apropiado. Se debe llevar a cabo un curso de medio día para familiarizarlos con los requisitos definidos en la nueva política de seguridad informática, los recursos organizacionales existentes y las mejores maneras de manejar una variedad de problemas, tales como fallas en la electricidad, intrusiones de hackers y virus de computadores. También se recomienda un manual para coordinadores locales de seguridad informática. Para mayor

información acerca de las fuentes de información que se podrían incluir en estos entrenamientos, ver Apéndice B, “[Lista de Publicaciones Periódicas Sobre Seguridad Informática](#). ”

Preparar y Dictar un Curso Básico de Adiestramiento en Seguridad Informática

—Un curso básico de adiestramiento se debería preparar y presentar a todos los empleados de la Empresa X. El documento de políticas puede constituir la fuente original de ideas para un curso de adiestramiento y de creación de conciencia. Se debería hacer referencia a otros tipos de información, tales como códigos corporativos de conducta, en el momento de preparar un curso. Después de que el curso haya sido presentado varias veces, se puede renovar, grabar en una cinta o en un software para adiestramiento asistido por computadores. En algunos casos, diferentes tipos de público pueden necesitar cursos diferentes. Los diferentes tipos de público pueden contemplar nuevos contratados en etapa de orientación, los empleados actuales con necesidad de más adiestramiento, los administradores de sistemas, los administradores de redes y los que puedan ser designados como coordinadores de seguridad informática, y los analistas de sistemas, los programadores de sistemas, los gerentes de proyectos relacionados con sistemas, el personal que garantiza la calidad de los sistemas y demás personal técnico que no será parte de los coordinadores de seguridad informática. Para mayor información en cuanto a la preparación de cursos de adiestramiento, ver “[Audiencia Definida Como Objetivo](#)” en la página 30.

Desarrollar Políticas de Seguridad Informática Específicas para Ciertas Aplicaciones—Algunas aplicaciones muy confidenciales necesitarán políticas y procedimientos específicos. Ahora que se ha elaborado la nueva política de seguridad informática, se deben desarrollar políticas y requisitos más específicos para sistemas de aplicaciones de alto riesgo. Algunos ambientes de computación, no sólo el de las aplicaciones, tal como el del comercio electrónico en Internet, pueden necesitar políticas y procedimientos más detallados. La jerarquía conceptual descrita a continuación se puede utilizar para describir el enlace entre estas aplicaciones específicas y la nueva política de seguridad informática. Para mayor información acerca de políticas detalladas y específicas, ver “[Objetivos y Alcance de las Políticas](#)” en la página 31.

Desarrollar una Jerarquía Conceptual de los Requisitos de Seguridad Informática—El área de seguridad informática es compleja, y esta complejidad se hace evidente en los varios documentos que definen los requisitos en seguridad informática. En muchas organizaciones, esto implica normas, lineamientos, políticas, procedimientos y arquitecturas. Una política general sobre seguridad informática debería estar al comienzo de una jerarquía conceptual, seguida de documentos de políticas relativas a las aplicaciones. Los documentos de normas, lineamientos, procedimientos y

otros, deberían estar bajo el control de la declaración de la política general de seguridad informática que se aplique a toda la organización. Una jerarquía conceptual debería indicar cuándo se aplican ciertos documentos, cuáles documentos deberían tener mayor importancia en el momento de un conflicto, y cuáles documentos están vigentes y cuáles no. Esta jerarquía conceptual será útil en los objetivos de adiestramiento y para crear conciencia, y pueden ser publicados en la página Intranet de seguridad informática de la Empresa X. Para mayor información para la creación de una jerarquía, ver “[Políticas de Seguridad Informática](#)” en la página 5.

Asignar Propiedad y Custodia de la Información—La propiedad por parte de la gerencia de tipos específicos de información se debería asignar de conformidad con los requisitos definidos en el nuevo documento de políticas de seguridad informática. Una vez asignados los roles de propiedad, se deberían asignar los roles de custodia. En muchos casos, estos esfuerzos constituirán una transición natural para la recopilación en el diccionario de datos corporativos, un sistema de manejo de documentos electrónicos o un proyecto similar. Para mayor información acerca de la asignación de propiedad, ver “[Propiedad de la Información](#)” en la página 42 y “[Custodio de la Información](#)” en la página 49.

Establecer un Comité de Gestión de la Seguridad Informática—Para supervisar las variadas iniciativas en cuanto a seguridad informática que actualmente se llevan a cabo, se debe conformar un comité con gerentes de nivel medio de cada una de las divisiones de la Empresa X. Este comité garantizará que las actividades vigentes de seguridad informática están en línea con los objetivos del negocio. Dicho comité actuará como el ente evaluador de las propuestas, antes de presentarlas a la consideración de la alta gerencia. Normalmente el comité se reúne trimestralmente, y no proporcionará ninguna asistencia técnica al departamento de Seguridad Informática. Para mayor información en cuanto a los comités, ver “[Comité de Gestión de Seguridad Informática](#)” en la página 41. Una declaración de misión y otros aspectos relacionados también se pueden ubicar en el libro *Roles y Responsabilidades en Seguridad Informática*.

Desarrollar un Documento sobre la Arquitectura de la Seguridad Informática—Aun cuando las reglas básicas de seguridad informática estén especificadas en

un documento de políticas, en la mayoría de los casos existe una necesidad de integrar una visión general al momento de diseñar un sistema de seguridad. Mientras más grande es una organización, mayor será la necesidad de un documento como éste, ya que estas organizaciones tienden a ser mucho más complejas. Una arquitectura debe especificar los controles que van a ser utilizados en la actualidad y en el futuro, y suministrar un plan para la migración de controles a ser adoptados en el futuro próximo. Algunas organizaciones también utilizan un documento de arquitectura como el sitio para especificar los productos y los proveedores autorizados de seguridad informática. Una arquitectura maneja las interfaces entre los sistemas, las normas técnicas y otras consideraciones técnicas que no se incluyen en las políticas. Para mayor información en cuanto a la arquitectura de la seguridad informática, ver “[Arquitectura de Sistemas para Registro de Actividades](#)” en la página 381.



Apéndice J CONVENIO DE CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Se debe presentar una copia firmada de este formulario con todas las solicitudes de autorización de un nuevo identificador de usuario, de autorización de cambios en los privilegios asociados con un identificador de usuario vigente, o de re-autorización periódica de un identificador de usuario vigente. La gerencia de la Empresa X no aceptará modificaciones de los términos y condiciones de este acuerdo.

Nombre Impreso del Usuario

Departamento y Número telefónico del Usuario

Dirección Física del Usuario y Dirección del Correo Electrónico

Yo, el usuario, convengo en tomar todas las precauciones razonables para garantizar que la información interna de la Empresa X, o la información que haya sido confiada a la Empresa X por terceros, tales como clientes, no será divulgada a personas no autorizadas. Al término de mi relación laboral o contrato con la Empresa X, convengo en devolver a la Empresa X toda la información a la cual haya tenido acceso por mi posición dentro de la Empresa X. Entiendo que no estoy autorizado a utilizar dicha información para objetivos personales, ni que tengo la libertad de suministrar dicha información a terceros sin la autorización por escrito del gerente interno de la Empresa X que haya sido designado Propietario de la información.

Tengo acceso a una copia del Manual de Políticas de Seguridad Informática de la Empresa X, he leído y entendido el manual y entiendo el impacto que tiene sobre mi trabajo. Como condición para continuar la relación laboral con la Empresa X, convengo en seguir las políticas y demás requisitos expresados en dicho manual. Entiendo que el incumplimiento de dichas condiciones generará acciones disciplinarias que incluyen la suspensión de los privilegios informáticos, el despido de la Empresa X y posibles acciones judiciales.

Estoy de acuerdo en escoger una contraseña difícil de adivinar, tal como está descrito en el Manual de Políticas de Seguridad Informática de la Empresa X, estoy de acuerdo en no compartir dicha contraseña y estoy de acuerdo en no escribir dicha contraseña en ninguna parte, a menos que sea irreconocible.

Asimismo, convengo en reportar inmediatamente cualquier violación o sospecha de violaciones de las políticas de seguridad informática al director del departamento de Seguridad Informática (al XXX-XX-XXXX).

Nombre Impreso del Usuario

Apéndice K DECLARACIÓN DE RESPONSABILIDAD SOBRE LA TARJETA DE IDENTIDAD

Yo, el suscrito, acuso recibo de una tarjeta de identidad con contraseña dinámica (en lo sucesivo, "la tarjeta"). Entiendo que esta tarjeta proporciona acceso a los sistemas informáticos de la Empresa X y a la información restringida almacenada en los mismos. Entiendo que los privilegios de acceso que acompañan a esta tarjeta pueden ser revocados en cualquier momento por la gerencia de la Empresa X, si piensan que no he seguido los lineamientos de la Declaración de las Políticas de Seguridad Informática, o si mi relación laboral con la Empresa X por cualquier razón se termina o se suspende. He leído y entendido el material que contiene la Declaración de las Políticas de Seguridad Informática y convengo en seguir estas reglas cada vez que utilice la información o los sistemas informáticos de la Empresa X.

Entiendo que esta tarjeta es exclusivamente para mi uso personal en el desempeño de mis actividades en la Empresa X, y prometo no compartirla o los privilegios informáticos que proporciona con ninguna otra persona. Convengo en no escribir o guardar el número de activación de la tarjeta de identificación personal sobre cualquier cosa que se encuentre cerca de la tarjeta.

Convengo en reportar inmediatamente al departamento de Seguridad Informática el hecho de que mi tarjeta haya sido robada o extraviada, o de que sospecho de que haya sido robada o extraviada. Estoy de acuerdo en entregar la tarjeta en el momento de que cese mi relación laboral con la Empresa X. En ese momento, convengo además en entregar al personal de la Empresa X la información y el equipo de computación y de comunicaciones que me haya sido suministrado para poder realizar mi trabajo.

Firma del Empleado y Fecha

Nombre Impreso del Empleado y Número de Empleado

Apéndice L DECLARACIÓN DE ACEPTACIÓN DE RIESGO

CUÁNDO UTILIZAR ESTE FORMULARIO

Este formulario debe emplearse cuando:

- se sabe que un sistema informático, un sistema de comunicaciones o una unidad de la organización no está cumpliendo las políticas de seguridad informática o normas de la Empresa X, y
- el gerente correspondiente no tiene intenciones de lograr cumplimiento cabal dentro de un período de tres meses.

Si la situación de incumplimiento va a continuar, la evaluación de riesgo breve respecto de la situación de incumplimiento debe actualizarse anualmente, las aprobaciones deben obtenerse anualmente, y este formulario debe estar firmado por el gerente correspondiente anualmente. Cada año, el gerente correspondiente debe regresar una copia firmada de este formulario al gerente de Seguridad Informática, quien lo guardará en sus archivos.

DECLARACIÓN DE ACEPTACIÓN DE RIESGO

Respecto de política o norma N°:

Relativo al tópico:

Entiendo que se espera el cumplimiento de las políticas y normas de seguridad informática de la Empresa X de parte de todas las unidades organizacionales, y de todos los sistemas informáticos y de comunicaciones. He leído la política o norma mencionada anteriormente y mi opinión es que el(los) control(es) allí descrito(s) no debería(n) requerirse para los siguientes:

- unidad organizacional
 sistema informático
 sistema de comunicaciones

(dibuje un círculo en la opción correspondiente y describa):

También entiendo que la deficiencia en los controles en un sistema conectado a una red puede poner en peligro otros sistemas informáticos, porque datos erróneos pueden ser heredados, o porque se puede crear un conducto a través del cual puede entrar un intruso a los sistemas de la Empresa X. Entiendo igualmente que el incumplimiento en esta instancia puede afectar adversamente la moral, o la disposición del personal asociado a otros sistemas para cumplir las normas y políticas de seguridad informática.

Entiendo que las excepciones a las normas y políticas de seguridad informática son adecuados sólo si:

- afectan adversamente el logro de las metas de la Empresa X, o
 causan un impacto financiero adverso que no podría ser compensado por el riesgo reducido del cumplimiento. Creo que se debe hacer una excepción en este caso porque:
-
-

He preparado, o he pedido a un integrante de mi equipo que prepare, una evaluación escrita de los riesgos asociados al incumplimiento de la norma o política mencionada. Este análisis de riesgo ha sido revisado y aprobado por el gerente del departamento de Seguridad de Sistemas Informáticos y el gerente de Auditoría Interna.

Acepto la responsabilidad personal de esta situación de incumplimiento de las normas y políticas de seguridad informática. Esta responsabilidad personal no significa ser financieramente responsable de las pérdidas que puedan ocurrir como resultado de este incumplimiento. La responsabilidad personal sí significa que mi evaluación de desempeño, mi salario y bonos, y mi posición de empleo continuo con la Empresa X, pueden verse en peligro o dañarse si ocurre una pérdida importante por esta situación de incumplimiento.

También entiendo que esta excepción vencerá al año de haber sido obtenidas las autorizaciones.

Firma de Gerente Responsable

Nombre en Letra de Molde del Gerente Responsable

Fecha Firmado

Apéndice M ACUERDO SIMPLE DE CONFIDENCIALIDAD

Este acuerdo de confidencialidad se celebra el _____ (fecha), entre la Empresa X, y _____ (nombre de la organización), que conjuntamente con sus subsidiarias y filiales será denominada en lo sucesivo individual y colectivamente como el "Receptor", Empresa X y el receptor acuerdan lo siguiente:

1. Empresa X creó y es Propietaria y desarrolladora de una idea para un nuevo producto (en lo sucesivo, el "Sistema"). Al divulgarle esta información, Empresa X no otorga al Receptor ninguna licencia ni derecho, por implicación o de alguna otra manera, para el uso de esta información para propósito alguno distinto de los fines específicos de negocios de la Empresa X, tal como se definen en los convenios escritos a negociar por separado.
2. El Receptor reconoce que el Sistema y toda su documentación, inclusive sin limitantes de las descripciones del Sistema o sus partes componentes, todas las maquetas del producto, sus prototipos, muestras, especificaciones técnicas, datos de entrada, conocimientos, ideas nuevas y diferentes relacionadas con el producto, tecnología, o todo o cualquier cosa que se derive de lo anterior (los cuales, individual y colectivamente, se denominan en lo sucesivo la "Información Propietaria") son valiosos, confidenciales y propiedad de la Empresa X.
3. Empresa X y el receptor desean discutir arreglos y relaciones de negocios mutuamente beneficiosos y que de alguna manera tienen que ver, o están relacionados con el Sistema. El Receptor reconoce que la divulgación de esta información constituye consideración para este convenio porque desea lograr la oportunidad de hacer negocios con Empresa X. El Receptor conviene en no utilizar la Información Propietaria para su propio uso o para cualquier otro fin excepto evaluar si desea llevar a cabo una relación de negocios con Empresa X o, de ser necesario, continuar dicha relación. El Receptor también conviene en manejar todos sus trabajadores que entren en contacto con la Información Propietaria de tal manera que las obligaciones y tareas aquí descritas sean de estricto cumplimiento.
4. El Receptor conviene en mantener la Información Propietaria en estricta confidencia. El Receptor también conviene en no reproducir, transcribir o divulgar la Información Propietaria a terceros sin el permiso escrito previo de Empresa X. El Receptor también conviene en no hacer, haber hecho, usar, distribuir o vender para sus propios fines o para cualquier otro fin distinto de aquel en nombre de Empresa X, cualquier producto que incorpore la Información Propietaria. El Receptor además conviene en devolver con prontitud todas las copias, traducciones, transformaciones y derivados de tal información a Empresa X al término de sus discusiones o asuntos de trabajo con el Sistema.

5. Las obligaciones impuestas por este convenio no se aplicarán a cualquier información que sea:
 - Recibida legítimamente de un tercero sin restricciones respectivas de divulgación, y que pueda ser documentada como tal.
 - Desarrollada independientemente sin acceso a la Información Propietaria.
 - Públicamente disponible por medios legales del Receptor.
 - Ya conocida al Receptor como se evidencia a través de documentación de terceros con fecha anterior a la fecha de divulgación de la Información Propietaria.
 - Aprobada para publicación por representante autorizado de Empresa X.
6. Este convenio reemplaza todos los convenios existentes, escritos o no, celebrados entre el Receptor y Empresa X a este respecto.
7. El Receptor conviene que, en caso de incumplimiento, Empresa X tendrá derecho a un amparo judicial para forzar el cumplimiento de los términos y condiciones de este convenio, y para proteger su Información Propietaria. El Receptor además conviene en aceptar la búsqueda por parte de Empresa X de otras acciones o remedios ante la ley, por cualquier incumplimiento o amenaza de incumplimiento de los términos de este convenio, inclusive sin limitantes de la recuperación de daños.
8. Si uno o más de los términos de este convenio llegase a ser considerado no válido, ilegal o no cumplible en cualquier otro aspecto, no se afectará la intención general del convenio, ni se afectará el grado de vinculación de los otros términos restantes, ni se interferirá con el forzoso cumplimiento de la responsabilidad de satisfacer los otros términos de este convenio. Este convenio se hace en concordancia con las leyes de [insertar jurisdicción correspondiente].
9. Los términos de este convenio estarán vigentes durante cinco años a partir del momento cuando El Receptor reciba la información de Empresa X. Cada vez que Empresa X proporcione nueva información confidencial al Receptor, el período durante el cual esta información debe mantenerse confidencial continuará durante cinco años desde ese momento. La terminación de la relación de trabajo propuesta o real entre El Receptor y Empresa X no invalida de manera alguna la naturaleza vinculante de este convenio o el período durante el cual estará vigente.
10. La persona abajo firmante por El Receptor asegura ser un representante autorizado y/o ejecutivo corporativo de la organización del Receptor.

Firma del Ejecutivo del Receptor y Fecha

Nombre en Letra de Molde del Ejecutivo Firmante

Ejecutivo de Empresa X y Fecha

Apéndice N INDICE DE NUEVAS POLÍTICAS

Las siguientes políticas han sido agregadas al Manual *Políticas de Seguridad Informática - Mejores Prácticas Internacionales* desde la última versión. Esta lista tiene

el propósito de ayudar a aquéllos que poseen la licencia de la versión anterior y desean actualizar sus declaraciones de política con enfoques sólo en las nuevas.

Tabla N-1: Nuevas Políticas

Número de la Política	Título de la Política
4.01.03.03	“Enfoque Gerencial de la Seguridad”
4.01.03.04	“Evaluaciones de Riesgos”
4.01.03.08	“Autorización para Cambios de los Sistemas Informáticos”
4.01.03.19	“Propiedad Predeterminada de la Información”
4.01.04.01	“Control de Nuevas Tecnologías”
4.01.06.01	“Divulgación de Productos de Seguridad Informática”
4.01.06.02	“Divulgación Pública de Información Empresarial”
4.02.01.02	“Privilegios de Trabajadores Temporales”
4.02.01.04	“Anotaciones de los Consultores”
4.02.02.04	“Manejo de la Información al Finalizar el Contrato”
4.02.02.05	“Prohibición de Invasión de Privacidad a Través de Terceros”
4.02.02.07	“Divulgación de las Relaciones con Proveedores”
4.02.02.13	“Medidas de Seguridad en Organizaciones de Terceros”
4.02.02.14	“Política de Seguridad del Tercero”
4.03.01.01	“Reportes Independientes Sobre Controles”
4.03.01.02	“Software del Proveedor de Servicios de Aplicaciones”
4.03.01.03	“Proveedor Alternativo de Procesamiento”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
4.03.01.05	“Planes para el Retorno de Sistemas de Producción Manejados por Terceros”
4.03.01.06	“Cortafuegos y Servidores Compartidos Externamente”
4.03.01.07	“Acceso a la Información Manejada por Contratista Externo”
4.03.01.08	“Decisiones Sobre Control de Acceso”
4.03.01.10	“Situación Financiera de Contratista Externo”
4.03.01.11	“Procesos de Producción Manejados por Compañías Extranjeras”
5.02.01.04	“Clasificación Cerrada de Datos en Dos Categorías”
5.02.01.05	“Clasificación Abierta de Datos en Dos Categorías”
5.02.01.08	“Etiquetas Incorrectas de Clasificación de Datos”
5.02.01.21	“Desclasificación de Archivos Secretos”
5.02.01.22	“Información y Software Esenciales”
5.02.02.01	“Retención de Datos en Grupos de Archivos”
5.02.02.03	“Nombres de los Sistemas de Computación”
5.02.02.33	“Divulgación de Información Desclasificada”
6.01.02.12	“Pruebas con Polígrafos”
6.01.02.17	“Revisión de Antecedentes de No Empleados”
6.01.02.19	“Antiguos Hackers y Delincuentes Reformados”
6.01.04.04	“Informantes Internos”
6.01.04.05	“Inteligencia Competitiva”
6.02.01.01	“Exámenes Sobre las Políticas”
6.03.01.06	“Bromas en Seguridad Informática”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
6.03.01.10	“Severidad de los Incidentes Reportados”
6.03.01.12	“Alternativas para el Reporte de Violaciones y Problemas”
6.03.01.15	“Identidad del Informante de Violaciones y Problemas”
6.03.01.19	“Reportes de Brechas de Seguridad a Terceros”
6.03.01.21	“Reporte de Eventos Cuestionables”
6.03.01.23	“Contacto con las Autoridades Policiales”
6.03.02.04	“Discusiones Sobre Debilidades y Vulnerabilidades en la Seguridad”
6.03.02.05	“Reporte de Vulnerabilidades en la Seguridad”
6.03.03.02	“Divulgación de Vulnerabilidades”
6.03.05.05	“Despidos Bajo Coacción”
7.01.01.02	“Plan de Seguridad Física”
7.01.02.07	“Entradas Individuales”
7.02.01.07	“Infraestructura de Respaldo para Centro de Datos”
7.02.03.01	“Cables Eléctricos y de Telecomunicaciones”
7.02.04.04	“Retención de Hardware y Software”
7.02.05.01	“Autorización de Uso de Equipo Fuera de Sede”
7.03.01.03	“Manejo de Información en Otros Turnos”
7.03.02.02	“Etiquetas Anti-Robo”
8.01.01.03	“Documentación de las Aplicaciones de Producción”
8.01.05.02	“Separación de Tareas en Tecnología Informática”
8.01.06.01	“Riesgos y Expectativas de Contratistas”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
8.02.02.01	“Configuración del Sistema”
8.02.02.03	“Evaluación de Nuevas Tecnologías”
8.03.01.01	“Acceso de Sistemas a la Red”
8.03.01.17	“Rastreo de Virus en Archivos de Respaldo”
8.03.01.23	“Descarga de Software por Internet”
8.04.01.05	“Archivos de Respaldo en Sede”
8.04.01.22	“Formularios de Papel Almacenados Fuera de Sede”
8.05.01.04	“Revisión de Conexiones Remotas”
8.05.01.05	“Control de Tráfico en Internet”
8.05.01.11	“Herramientas para Evaluar Integridad”
8.05.01.16	“Sistemas de Detección de Intrusos Basados en Servidor”
8.05.01.18	“Acceso del Administrador al Cortafuego de Internet”
8.05.01.44	“Redes Inalámbricas”
8.05.01.45	“Puertas de Enlace a Redes Inalámbricas”
8.06.03.09	“Copia Maestra de Datos Críticos de Producción”
8.07.01.05	“Contratos en Línea con Intercambio de Papel y Firmas”
8.07.02.01	“Entrega por Terceros de Información Secreta”
8.07.03.01	“Obtención de Información desde Archivos Cookie”
8.07.03.02	“Clasificación de Contenido y Protección de la Privacidad”
8.07.03.04	“Colocación de Clientes y Prospectos en Listas de Correos”
8.07.03.07	“Confirmación de Cambio Solicitado por Cliente”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
8.07.03.21	“Números de Tarjeta de Crédito Inactivos”
8.07.04.13	“Cifrado de Correo Electrónico del Cliente”
8.07.04.24	“Revisión de Correo Electrónico y Pies de Página”
8.07.04.25	“Pie de Página de Correo Electrónico Saliente”
8.07.04.28	“Correo Electrónico del Departamento de Ventas”
8.07.04.35	“Anexos de Correo Electrónico No Esperados”
8.07.05.13	“Información Confidencial Vía Fax — Discado Rápido”
8.07.05.40	“Cuentas Personales en un Proveedor de Servicios de Internet”
8.07.05.43	“Ejecución de Código Móvil”
8.07.06.07	“Estaciones de Trabajo de Acceso Público”
8.07.06.11	“Mensajes de Delincuentes o Terroristas”
8.07.06.14	“Grupos de Discusión en Internet”
8.07.06.26	“Preguntas sobre Seguridad en Internet”
8.07.06.45	“Cambios en Contenido de Sitio Web en Internet”
8.07.06.46	“Ataques a Páginas Web”
8.07.06.47	“Almacenamiento de Información Financiera de Clientes”
8.07.06.48	“Nombre de Dominio en Internet”
8.07.06.49	“Respuestas a Comandos en Servidores Internet”
8.07.06.50	“HTML del Sitio Web”
8.07.06.52	“Información Secreta en Intranet”
8.07.07.01	“Grabación de Comunicaciones en Internet”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
9.01.01.08	“Base de Datos Centralizada de Controles de Acceso”
9.01.01.09	“Software Intérprete de Líneas de Comando”
9.01.01.18	“Información de Asuntos Legales”
9.01.01.26	“Autorización de Divulgación de Información”
9.01.01.30	“Creación de Herramientas de Seguridad”
9.02.01.02	“Identificador de Usuario No Anónimo”
9.02.01.12	“Autorización de Solicitud de Acceso al Sistema”
9.03.01.15	“Uso de Contraseñas por Terceros”
9.04.01.05	“Acceso a la Red Interna”
9.04.01.09	“Bloqueo de Acceso a Sitios Ajenos al Negocio”
9.04.01.10	“Descargas Grandes desde Internet”
9.04.03.01	“Contraseñas de Acceso Remoto”
9.04.03.02	“Autentificación de Usuario Mediante Dos Factores”
9.04.05.01	“Acceso al Puerto de Diagnóstico”
9.05.01.01	“Seguridad Física del Terminal”
9.04.08.01	“Zonas de Seguridad de la Red”
9.04.09.01	“Cortafuegos de Computadores Personales y Estaciones de Trabajo”
9.05.03.02	“Credenciales Portátiles de Identificación”
9.05.04.03	“Contraseñas para Computadores Conectados a la Red”
9.05.04.04	“Longitud de Contraseña de Acuerdo con la Función”
9.05.04.19	“Información de Control de Acceso en Cookies”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
9.06.01.12	“Divulgación de Registro del Sistema y Seguimientos de Auditorías”
9.06.02.01	“Servidores para Aplicaciones Críticas”
9.07.01.06	“Registros de Acceso a Información Privada”
9.07.02.12	“Monitoreo de Actividad en Internet”
9.08.01.04	“Uso de Computadores Portátiles”
10.01.01.02	“Propuestas para Desarrollar Sistemas Internos”
10.01.01.05	“Principios de Codificación de Aplicación”
10.02.02.16	“Archivos y Almacenamiento Temporales”
10.02.04.01	“Controles de Datos de Salida”
10.03.01.01	“Versiones de Software para Firmas Digitales y Cifrado de Archivos”
10.03.02.10	“Protección de Mensajes Cifrados”
10.03.05.04	“Vigencia de los Certificados Digitales”
10.03.05.22	“Almacenamiento de Claves de Cifrado y Firmas Digitales”
10.03.05.27	“Controles en la Operación de Recuperación de Claves”
10.04.01.01	“Prueba del Sistema de Aplicaciones de Negocios”
10.04.03.02	“Acceso a Programas e Información de Producción”
10.05.01.19	“Documentación de los Controles de Cambios”
10.05.02.01	“Configuración del Sistema Operativo”
10.05.02.02	“Parches de Software, Arreglos y Actualizaciones”
10.05.05.01	“Desarrollo de Software por Terceros”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
11.01.01.02	“Accesibilidad del Plan de Contingencia”
11.01.02.03	“Análisis del Impacto sobre el Negocio”
11.01.05.02	“Rotación del Personal Fuera de Sede”
11.01.05.05	“Prueba de Números Telefónicos”
11.01.05.06	“Roles en la Planificación de Contingencias y Recuperación de Sistemas”
12.01.01.01	“Reglamentos y Requisitos”
12.01.02.02	“Sistemas de Producción y Herramientas de Software”
12.01.02.18	“Libros Electrónicos con Derecho de Autor”
12.01.03.06	“Almacenamiento de Registros Vitales”
12.01.03.12	“Retención de los Datos de Transacciones con Aplicaciones”
12.01.04.01	“Efectos Personales y Comunicaciones Privadas”
12.01.04.02	“Recopilación de Datos Personales Bajo Pretextos”
12.01.04.11	“Consentimiento para la Recopilación de Información Privada”
12.01.04.36	“Compartir Información Privada”
12.01.04.37	“Divulgación de Información Privada a Organizaciones Contratadas”
12.01.04.39	“Divulgación de Datos Personales”
12.01.04.59	“Registro del Acceso a la Información Privada”
12.01.04.67	“Inteligencia de Números de Cuentas”
12.01.04.71	“Recordatorio de Política de Privacidad”
12.01.04.73	“Control del Individuo sobre el Uso de sus Datos Personales”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
12.01.04.74	“Uso de Información Específica Respecto de la Ubicación”
12.01.04.76	“Eliminación de la Información del Cliente o Prospecto”
12.01.04.78	“Compartir Información Personal”
12.01.04.79	“Transferencia de la Información sobre Clientes”
12.01.04.80	“Transferencia de Datos Personales”
12.01.04.84	“Lista de Tipos de Información de Producción Disponibles para Empleados”
12.01.04.86	“Cifrado de Correo Electrónico Privado”
12.01.04.93	“Distribución de Políticas de Privacidad”
12.01.05.05	“Acceso de Usuarios a Internet”
12.01.05.06	“Clasificación del Uso Aceptable de Internet”
12.01.05.10	“Tiempo de Acceso Personal a Internet”
12.01.05.12	“Identificadores de Usuario Empleados en Actividades Abusivas”
12.01.07.02	“Fuentes de Evidencia Digital”
12.01.07.09	“Investigaciones Policiacas o Legales”
12.01.07.10	“Participación en Procedimiento Legal”
12.01.07.11	“Provisión de Información en Procedimientos Legales”
12.01.07.12	“Contactos con Autoridades Judiciales”
12.01.07.13	“Reportes Sobre Situación de la Investigación”
12.01.07.15	“Proceso de Análisis Forense”
12.01.07.16	“Investigaciones de Seguridad Informática”
12.01.07.17	“Equipos de Investigación de Seguridad Informática”

Tabla N-1: Nuevas Políticas (Continued)

Número de la Política	Título de la Política
12.01.07.18	“Investigaciones Internas y Solicitudes Oficiales”
12.01.07.19	“Detalles de Investigaciones de Intrusiones”



Apéndice O INDICE DE NUEVOS NOMBRES DE POLÍTICAS

La mayoría de los títulos de las políticas incluidas en el Manual *Políticas de Seguridad Informática - Mejores Prácticas Internacionales* han sido modificados desde la última versión. La siguiente lista contiene los nombres dados a las políticas en la versión 8 de este

manual, conjuntamente con el nuevo nombre o título que recibe en la presente versión. Cada una de las políticas aparece en el orden en que fueron publicadas en la versión 8.

Tabla O-1: Indice de Nuevos Nombres de las Políticas

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1	Longitud Mínima de Contraseñas	9.05.04.01	“Longitud Mínima de Contraseñas”
2	Longitud Mínima de Contraseñas Restringida por Limitaciones del Sistema	9.05.04.02	“Restricción a la Longitud Mínima de las Contraseñas”
3	Se Requieren Contraseñas Difíciles de Adivinar	9.03.01.01	“Estructura de las Contraseñas”
4	Contraseñas Cíclicas Prohibidas	9.03.01.02	“Contraseñas Cíclicas”
5	Contraseñas del Usuario No deben Reusarse	9.05.04.05	“Reutilización de Contraseñas”
6	Contraseñas Deben Contener Caracteres Alfabéticos y No Alfabéticos	9.05.04.06	“Caracteres de las Contraseñas”
7	Contraseñas Deben Contener Caracteres en Mayúsculas y en Minúsculas	9.05.04.07	“Mayúsculas y Minúsculas en Contraseñas”
8	Base para Contraseñas Generadas por el Sistema	9.05.04.09	“Semilla para Contraseñas Generadas por el Sistema”
9	Contraseñas Pronunciables Generadas por el Sistema	9.05.04.10	“Contraseñas Generadas por el Sistema”
10	Almacenamiento de Contraseñas Generadas por el Sistema	9.05.04.11	“Emisión y Almacenamiento de Contraseñas Generadas por el Sistema”
11	Inicialización de Materiales para la Generación de Contraseñas	9.05.04.12	“Materiales para la Generación de Contraseñas”
12	Protección de Algoritmos Generadores de Contraseñas	9.05.04.13	“Algoritmos Generadores de Contraseñas”
13	Archivo Histórico de Contraseñas Anteriores	9.05.04.08	“Histórico de Contraseñas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
14	Identificadores de Usuarios Anónimos	9.02.01.01	“Identificadores de Usuarios Anónimos”
15	Despliegue e Impresión de Contraseñas	9.05.04.14	“Visualización e Impresión de Contraseñas”
16	Contraseñas de Usuarios Deben Introducirse Dos Veces Si Estaban Enmascaradas	9.05.04.15	“Máscaras para Cambios de Contraseña”
17	Cambios Periódicos Forzados de Contraseñas	9.05.04.16	“Cambios Obligatorios de Contraseña”
18	Sincronización de los Intervalos de Cambios de Contraseñas en Distintas Plataformas	9.05.04.17	“Sincronización de los Intervalos de Cambios de Contraseñas”
19	Asignación de Contraseñas Vencidas	9.02.03.01	“Contraseñas Iniciales”
20	Contraseñas Iniciales Transmitidas a Usuarios Remotos por Medios Autorizados	9.02.03.02	“Transmisión de Contraseña Inicial”
21	Límite de Intentos Infructuosos Consecutivos de Introducir Contraseña	9.05.02.01	“Intentos de Introducir Contraseña”
22	Proceso Unico de Inicio de Sesión	9.05.03.01	“Mecanismo Unico de Acceso”
23	Todas las Estaciones de Trabajo Deben Tener Protección de la Inicialización Basada en Contraseña	9.05.02.02	“Protección de la Reinicialización Basada en Contraseña”
24	Contraseñas Nunca Legibles Cuando Estén Fuera de las Estaciones de Trabajo	9.05.04.18	“Contraseñas Legibles”
25	Contraseñas Fijas de Servicio al Cliente No Visualizadas por Sistemas de Empresa X	9.06.01.01	“Contraseñas de Servicio al Cliente”
26	Cambios de Contraseñas Fijas Confirmados por Correo Normal para Detectar Abuso	9.02.03.03	“Confirmación de Cambio de Contraseña Fija”
27	Protección de Contraseñas Enviadas por Correo	9.02.03.04	“Envío de Contraseñas por Correo”
28	Reregistro Obligatorio para Todos los Usuarios que Olviden Sus Contraseñas Fijas	9.02.03.05	“Contraseñas Fijas Olvidadas”
29	Reinicialización de Contraseña Despues de Desactivación Requiere Centro de Atención al Usuario	9.02.03.06	“Reinicialización de la Contraseña Posterior a la Desactivación”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
30	Almacenamiento de Contraseñas Legibles	9.03.01.03	“Almacenamiento de Contraseñas Legibles”
31	Cifrado de Contraseñas	9.05.04.20	“Cifrado de Contraseñas”
32	Incorporación de Contraseñas al Software	9.02.03.07	“Contraseñas en Software”
33	Prevención de la Recuperación de Contraseña	9.05.04.21	“Recuperación de Contraseñas”
34	Dependencia del Proceso de Autenticación del Usuario por Sistema Operativo	9.05.03.03	“Autentificación del Usuario por el Sistema Operativo”
35	Prohibición de Privilegios Especiales Asociados con Identificadores de Usuario o Contraseñas Secretas	9.06.01.02	“Identificadores de Usuario o Contraseñas Secretas”
36	Sistema de Control de Acceso con Contraseñas Individualizadas	9.05.04.22	“Contraseñas de Control de Acceso al Sistema”
37	Contraseñas Unicas para Cada Dispositivo Interno de la Red	9.04.07.01	“Contraseñas para los Dispositivos Internos de la Red”
38	Uso de Contraseñas de Presión	9.05.06.01	“Contraseñas de Presión”
39	Cambio de las Contraseñas Proporcionadas por el Proveedor	9.05.04.23	“Contraseñas Proporcionadas por Proveedores”
40	Requisito de Distintas Contraseñas en Distintos Sistemas	9.03.01.04	“Contraseñas en Distintos Sistemas”
41	Permiso Para Usar Misma Contraseña en Distintos Sistemas	9.03.01.05	“Contraseñas en Distintos Sistemas — Permiso”
42	Sospecha de Divulgación Obliga a Cambio de Contraseña	9.03.01.06	“Sospecha de Divulgación de Contraseña”
43	Cambios de Contraseñas Despues de Estar Comprometido Sistema Multiusuario	9.05.04.24	“Cambios de Seguridad Despues de Estar Comprometido el Sistema”
44	Anotar Contraseñas y Dejarlas Donde Otros Puedan Descubrirlas	9.03.01.07	“Divulgación Pública de Contraseñas”
45	Contraseñas Nunca Deben Anotarse Cerca de Dispositivos de Acceso Relacionados	9.03.01.08	“Proximidad de Contraseñas a Dispositivos de Acceso”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
46	No Almacenar Contraseñas Fijas en Programas de Mercado o Exploradores de Internet	9.03.01.09	“ Contraseñas en Software de Comunicaciones ”
47	Máquinas Controladas por Usuarios No Deben Emplear Cookies para Inicios Automáticos de Sesión	9.03.01.10	“ Cookies para Inicios Automáticos de Sesión ”
48	Tarjetas de Contraseñas Dinámicas No Deben Guardarse en Portafolios Portátiles	9.03.01.11	“ Tarjetas de Contraseñas Dinámicas ”
49	Números de Identificación Personal (PINs) Construidos Usando Reglas de Contraseñas	9.03.01.12	“ Números de Identificación Personal ”
50	Escritura de Contraseñas Usando Técnicas Seguras	9.03.01.13	“ Escritura de Contraseñas ”
51	Prohibición de Compartir Contraseñas	9.03.01.14	“ Contraseñas Compartidas ”
52	Usuarios Responsables de Todas las Actividades Que Involucren a sus Identificaciones Personales de Usuario	9.03.01.16	“ Identificadores Personales de Usuario — Responsabilidad ”
53	Cambio Obligatorio de Todas las Contraseñas Despues de Estar Comprometido el Sistema	9.02.03.08	“ Cambios de Contraseña Luego de Estar Comprometido el Sistema ”
54	Cambio Obligatorio de Todas las Contraseñas Despues de Estar Comprometida la Cuenta del Supervisor	9.02.03.09	“ Cambio de Contraseña de Usuario Privilegiado Comprometida ”
55	Prueba de Identidad en Persona para Obtener Contraseña	9.02.03.10	“ Autenticación de Contraseña en Persona ”
56	Cuándo y Cómo Pueden Administradores de Seguridad Divulgar Contraseñas	9.02.03.11	“ Divulgación de Contraseñas ”
57	Identificación Positiva Obligatoria para Uso del Sistema	9.02.03.12	“ Identificación Positiva para Uso del Sistema ”
58	Controles de Acceso para Sistemas Remotos Conectándose a Sistemas de Producción	9.04.03.03	“ Controles de Acceso para Sistemas Remotos ”
59	Identificadores de Usuario y Contraseña Obligatorias para Acceso a la Red	9.04.03.04	“ Acceso a la Red ”
60	Identificadores de Usuario Unica y Contraseña Obligatorios	9.02.01.03	“ Identificador Unico de Usuario y Contraseña Obligatorios ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
61	Divulgación de Información de Acceso Incorrecto	9.05.02.03	“Información de Inicio de Sesión”
62	Prohibición de Respuesta ante Error en Acceso	9.05.02.04	“Respuesta por Inicio Incorrecto de Sesión”
63	Mensaje de Seguridad en Acceso	9.05.02.05	“Mensaje de Advertencia en Inicio de Sesión”
64	Divulgación de Información en Mensaje de Acceso	9.05.02.06	“Información en Mensaje de Inicio de Sesión”
65	Mensaje de Red Obligatorio	9.05.02.07	“Mensaje de Inicio de Sesión en la Red”
66	Aviso de Ultima Fecha y Hora de Acceso	9.05.02.08	“Ultima Hora y Fecha de Inicio de Sesión”
67	Límite a Cantidad de Accesos Diarios Evita Uso No Autorizado	9.05.02.09	“Límite al Acceso Diario”
68	Prohibición de Sesiones Múltiples Simultáneas En Línea	9.05.03.04	“Sesiones Múltiples Simultáneas”
69	Proceso Automático de Cierre de Sesión	9.05.07.01	“Cierre de Sesión Automático”
70	Abandonar Sistemas Confidenciales sin Cerrar Sesión	9.03.02.01	“Sesiones Activas Desatendidas”
71	Cierre de Sesión en Computadores Personales Conectados a Redes	9.03.02.02	“Sistemas de Redes Desatendidos”
72	No se Pueden Almacenar o Usar Juegos en los Sistemas de Computación de la Empresa X	12.01.05.01	“Juegos en los Sistemas de Computación de la Organización”
73	Uso Personal de los Sistemas de Computación y de Comunicaciones	12.01.05.02	“Uso Personal de los Sistemas de Computación y de Comunicaciones”
74	Uso Personal Incidental Permisible de los Sistemas Empresariales	12.01.05.03	“Uso Personal Incidental de los Sistemas de Comunicación”
75	Uso Personal Razonable Consistente Con Normas Eticas Convencionales	12.01.05.04	“Uso Personal Razonable de los Sistemas de Computación y de Comunicaciones”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
76	Prohibición de Usos No Autorizados del Sistema	12.01.05.07	“Usos Inaceptables de los Sistemas de Computación y de Comunicaciones”
77	Prohibición de Usar Internet para Propósitos Personales	12.01.05.08	“Uso Personal de Internet”
78	Uso Personal de las Facilidades de Internet de la Empresa X Sólo en Tiempo Personal	12.01.05.09	“Uso Personal de los Servicios de Internet de la Organización”
79	Límite de Tiempo para Uso Personal y Actividades Prohibidas	12.01.05.11	“Restricciones al Uso Personal”
80	Usos Permisibles de la Información de la Empresa X	3.01.01.02	“Uso de la Información”
81	Otorgamiento de Identificador de Usuario a Terceros	4.02.01.01	“Identificadores de Usuario para Terceros”
82	Acceso de Terceros a Sistemas de Empresa X Requiere Contrato Firmado	4.02.02.01	“Términos y Condiciones para el Acceso de Terceros”
83	Al establecerse, los Identificadores de Usuario de Terceros Deben Tener Fecha de Vencimiento Definida	9.02.01.04	“Vencimiento de los Identificadores de Usuario para No Empleados”
84	Privilegios de Acceso a Sistemas de Información Terminan Cuando los Trabajadores Se Van	9.02.01.05	“Finiquito de los Privilegios de Acceso”
85	Límites de Tiempo para los Identificadores de Usuario y Período de Retención de Archivos Despues del Vencimiento	9.02.01.06	“Vencimiento de los Identificadores de Usuario”
86	Excepción de Responsabilidad por Daños a Datos y Programas	3.01.01.04	“Excepciones de Responsabilidad por Daños a Datos y Programas”
87	Acceso No Autorizado Obtenido Vía los Sistemas Informáticos de la Empresa X	9.01.01.01	“Actividades del Hacker”
88	Dónde Usar los Controles de Acceso a los Sistemas de Computación	9.06.01.03	“Controles de Acceso al Sistema de Computación”
89	Uso de los Asistentes Personales Digitales para la Información Empresarial	9.08.01.01	“Uso de Pequeños Computadores Portátiles”
90	No Mantener Información Confidencial en Asistentes Personales Digitales, Portátiles, Etc.	9.08.01.02	“Información Sensible en Pequeños Computadores”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
91	Todo Software Debe Estar Regulado por Software de Sistemas de Control de Acceso	9.01.01.02	“Regulación del Software”
92	Sistemas Que Requieren Paquete de Control de Acceso Basado en Contraseña	9.01.01.03	“Control de Acceso Basado en Contraseña”
93	Restricción de Privilegios Basada en Necesidad de Conocer	9.02.02.01	“Restricción de Privilegios — Necesidad de Conocer”
94	Restricción de Privilegios Basada en Necesidad de Retener	9.02.02.02	“Restricción de Privilegios — Necesidad de Retener”
95	Políticas Específicas de Acceso a la Información Deben Ser Preparadas	4.01.03.24	“Políticas de Acceso a la Información”
96	Propiedad de la Información Debe Ser Asignada	4.01.03.01	“Propiedad de la Información”
97	Sin Permiso de Lectura para Acceder a Información Confidencial	9.01.01.04	“Acceso de Lectura a Información Sensible”
98	Sin Permiso de Escritura para Acceder a Información Confidencial	9.01.01.05	“Acceso de Escritura a Información Sensible”
99	Verificación de Edad Obligatoria para Acceder a Material Adulto	9.06.01.04	“Acceso a Material Adulto”
100	Separación Entre Usuarios de Actividades y Datos	9.06.01.05	“Separación de Actividades y Datos”
101	Permisos de Archivo Predeterminados para Sistemas Conectados en Red	9.01.01.06	“Permisos Predeterminados de Archivo”
102	Existencia de Capacidad para Permitir Acceso No Significa Permiso para su Uso	9.06.01.06	“Capacidad de Acceso de Usuarios”
103	Los Identificadores de Usuario Deben Identificar a un Solo Usuario	9.02.01.07	“Identificadores de Usuarios Únicos”
104	Prohibidos los Identificadores de Usuario Basados en Cargos	9.02.01.08	“Identificadores de Usuario Genéricos”
105	Re-Utilización de Identificador de Usuario Único Está Prohibido	9.02.01.09	“Re-Utilización de Identificadores de Usuario”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
106	Norma de Creación para un Identificador Unico de Usuario en Todas las Plataformas	9.02.01.10	“Norma de Creación para Identificadores de Usuario”
107	Separación de Identificadores de Usuario para Sistemas Conectados a Internet y a Redes Internas	9.02.01.11	“Múltiples Identificadores de Usuario”
108	Uso Personal Exclusivo de Códigos de Acceso Tales Como Identificadores de Usuario y Tarjetas de Crédito	9.03.01.17	“Compartir Códigos de Acceso”
109.	Identificación Positiva Requerida para Iniciar Transacciones en el Computador	9.05.03.05	“Iniciación de Transacciones en Computadores”
110	Soporte para Tipos de Usuarios Privilegiados	9.02.0203	“Usuarios Especiales Privilegiados”
111	Restricción de Privilegios Especiales	9.02.02.04	“Privilegios Especiales en Sistema”
112	Administración Remota Restringida de Computadores Conectados a Internet	9.04.03.05	“Administración Remota”
113	Cantidad Límite de Identificadores de Usuarios Privilegiados	9.02.02.05	“Cantidad de Identificadores de Usuarios Privilegiados”
114	Dos Identificadores de Usuario Obligatorios para Todos los Administradores de Sistemas	9.02.02.06	“Identificador de Usuario Administrador”
115	Registro e Informes sobre Actividad de Identificadores de Usuarios Privilegiados	9.07.02.01	“Registros de Actividad de Identificadores de Usuarios Privilegiados”
116	Privilegios Predeterminados y Necesidad de Autorizaciones Explícitas Escritas	9.06.01.07.	“Privilegios Predeterminados de Usuario”
117	Autorizaciones Necesarias para Crear Identificador de Usuario y Asignar Privilegios	9.02.02.07	“Autorización de Identificador de Usuario y Privilegio”
118	Restricción de Privilegios de Terceros en Conexiones Entrantes e Internet	4.02.01.03	“Acceso Remoto de Terceros”
119	Control de Acceso Dependiente del Tiempo	9.05.08.01	“Control de Acceso Crono-Dependiente”
120	Revocación de Identificadores de Usuarios Inactivos y Privilegios Automáticos	9.02.01.13	“Privilegios de Identificadores de Usuarios Inactivos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
121	Denegación Predeterminada de Privilegios de Control de Acceso	9.01.01.07	“Mal Funcionamiento del Control de Acceso”
122	No Deben Establecerse Relaciones de Confianza entre Servidores Sin Permiso	8.05.01.01	“Relaciones de Confianza entre Servidores”
123	Revocación de Privilegios de Acceso	3.01.01.09	“Revocación de Privilegios de Acceso”
124	Acceso de Usuario Final a Comandos del Sistema Operativo	9.02.02.08	“Acceso a Comandos del Sistema Operativo”
125	Límites al Conocimiento de Usuarios Finales de Comandos y Capacidades del Sistema	9.06.01.08	“Comandos y Capacidades del Sistema”
126	Finiquito de Procesos o Sesiones del usuario y Eliminación de Archivos del Usuario	8.01.01.01	“Procesos, Sesiones y Archivos de Usuarios”
127	Prohibición de Pruebas de los Controles del Sistema Informático	9.03.01.18	“Prueba de los Controles del Sistema Informático”
128	Prohibición de la Explotación de las Vulnerabilidades de la Seguridad del Sistema	9.03.01.19	“Explotación de las Vulnerabilidades de la Seguridad del Sistema”
129	Selección de Recipiente para la Distribución de Poderosas Herramientas de Seguridad	9.05.05.01	“Selección de Herramientas de Seguridad”
130	Remoción de Software de Identificación de Vulnerabilidades Si No Se Usa	9.05.05.02	“Software de Identificación de Vulnerabilidades”
131	Limitación de la Funcionalidad de Poderosas Herramientas de Sistemas Informáticos	9.05.05.03	“Poderosas Herramientas de Sistemas Informáticos”
132	Privilegios para Modificar la Información de Producción	9.06.01.09.	“Privilegios Sobre la Información de Producción”
133	Proceso Controlado para la Modificación de la Información de Producción	10.02.02.01	“Modificación de la Información de Negocio de Producción”
134	Actualización de la Información de Producción por Personal Distinto de Producción	9.02.02.09.	“Actualización de Información de Producción”
135	Actualización de la Base de Datos Debe Hacerse Solamente por los Canales Establecidos	9.06.01.10	“Actualizaciones de la Base de Datos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
136	Control de Acceso Obligatorio para Todas las Aplicaciones de Producción Multiusuario	9.06.01.11	“Aplicaciones de Producción Multiusuario”
137	Privilegios del Personal Técnico y Control de Cambios al Sistema de Producción	10.04.03.01	“Privilegios del Personal Técnico”
138	Formularios Firmados Obligatorios para Emisión de Identificadores de Usuario	9.02.01.14	“Formularios para Identificadores de Usuario”
139	Convenciones de Nombramiento de Sistemas Multiplataforma	5.02.02.02	“Convenciones en Nombres”
140	Gestión de Seguridad para Todos los Computadores en Red	8.05.01.02	“Configuración de Seguridad”
141	Herramientas para Determinar Estado de Seguridad del Sistema	9.05.05.04	“Herramientas de Estado de Seguridad del Sistema”
142	Revisión Periódica y Reautorización de los Privilegios de Acceso de Usuario	9.02.04.01	“Reautorización de los Privilegios de Acceso de Usuario”
143	Recursos Humanos Envía Cambios en Situación de Trabajador a Administradores de Sistema	4.01.03.02	“Cambios en Situación del Trabajador”
144	Informe de Cambios en Tareas de Usuario a la Administración de Seguridad del Sistema	9.02.01.15	“Informe de Cambios en Situación de Empleados”
145	Usuarios Deben Informar a Administración de Sistemas Acerca de Cambios en Su Situación	9.02.01.16	“Cambios en Situación de Usuarios”
146	Mantenimiento de Base de Datos Maestra de Identificadores de Usuario y Privilegios	9.02.02.10	“Base de Datos Maestra de Identificadores de Usuario”
147	Transferencia de Tareas de Custodia de Información Despues de Cese de Relaciones Laborales	9.02.01.17	“Transferencia de Responsabilidad en Custodia”
148	Cronograma para Eliminar Archivos Luego de Cese de Relación Laboral	9.02.01.18	“Eliminación de Archivos de Trabajador Cesado”
149	Registros Obligatorios en Sistemas que Manejan Información Confidencial	9.07.01.01	“Registros en Sistemas y Aplicaciones Sensibles”
150	Registro de Teclas Usadas Obligatorio para los Identificadores de Usuarios Privilegiados en Sistemas de Producción	9.07.02.03	“Registro de Cada Tecla Presionada”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
151	Inclusión de Eventos Importantes Relativos a Seguridad en Registro del Sistema	9.07.01.03	“Registro de Eventos Importantes de Seguridad”
152	Registros del Sistema Deben Soportar Auditorías	9.07.01.11	“Registros de Auditoría en los Sistemas”
153	Responsabilidad y Seguimiento de Todos los Comandos Privilegiados del Sistema	9.07.02.04	“Responsabilidad y Seguimiento de Comandos Privilegiados del Sistema”
154	Contenido de Registros en Sistemas Que Ejecutan Aplicaciones de Producción	9.07.01.02	“Contenido de Registros en Aplicaciones de Producción”
155	Todos los Intentos de Acceso, Exitosos o No, Deben Registrarse	9.07.01.04	“Registro de Intentos de Acceso”
156	Contraseñas de Acceso No Deben Registrarse Excepto Cifradas	9.07.02.05	“Registro de Contraseñas”
157	Período de Retención Obligatorio de Registros	9.07.01.07	“Período de Retención de Registros”
158	Remoción Diaria de Registros de los Computadores Accesibles desde Internet	9.07.01.08	“Remoción de Registros de Computadores Accesibles desde Internet”
159	Registros de Actividades Relativas a Seguridad Iniciadas por Usuarios	9.07.01.05	“Registros de Eventos de Seguridad Iniciados Por Usuarios”
160	Retención de Registros de Privilegios de Control de Acceso	9.07.01.09.	“Retención de Registros de Privilegios de Control de Acceso”
161	Capacidad de Reconstrucción de Cambios a Información de Producción	9.07.02.02	“Capacidad de Reconstrucción de Cambios en Producción”
162	Sumas de Verificación Criptográficas para Detectar Modificaciones en los Registros del Sistema	9.07.02.06	“Controles para Modificaciones de los Registros del Sistema”
163	Información a Capturar Cuando Se Sospeche de Crimen Informático o de Abuso	12.01.07.01	“Evidencia de Delito o Abuso Informático”
164	Registros Obligatorios para la Rápida Reanudación de las Actividades de Producción	8.01.01.02	“Registros de Aplicaciones Críticas”
165	Arquitectura de Sistemas para el Registro de Actividades	9.07.01.10	“Arquitectura de Sistemas para Registro de Actividades”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
166	Sincronización del Reloj para el Registro Preciso de Eventos en la Red	9.07.03.01	“Sincronización del Reloj”
167	Registro de Todos los Faxes Entrantes y Salientes	8.07.05.01	“Registros de Faxes”
168	Resistencia de Registros a Desactivación, Modificación o Eliminación	9.07.02.07	“Desactivación, Cambio o Eliminación de Registros”
169	Escríptura de Registros a Medios de Almacenamiento Evita Alteración	9.07.02.08	“Medios de Almacenamiento de Sistemas de Producción”
170	Sistemas Accesibles Externamente Deben Emplear Registros Espejos Remotos	9.07.01.12	“Registros Espejos Remotos”
171	Firmas Digitales y Números Secuenciales Obligatorios para Registros del Sistema	9.07.02.09	“Protección de Registros del Sistema”
172	Rotación y Archivo de Registros del Sistema para Sistemas de Alta Seguridad	9.07.01.13	“Rotación y Archivado de Registros del Sistema”
173	Personas Autorizadas para Ver Registros	9.07.02.10	“Acceso a Registros”
174	Revisión Pronta y Regular de Registros del Sistema	9.07.02.11	“Revisión de Registros del Sistema”
175	Notificación a Usuarios Acerca de Registro de Violaciones de la Seguridad	9.07.01.14	“Conciencia del Usuario Sobre Registros de Violaciones de Seguridad”
176	Usuarios No Deben Intentar Erradicar Virus de sus Computadores	8.03.01.02	“Eradicación de Virus de Computadores”
177	Eradicación de Virus Requiere de Soporte de Administrador del Sistema	8.03.01.03	“Eradicación de Virus por Administradores del Sistema”
178	Prohibición de Descargar Software de Sistemas de Terceros	8.03.01.04	“Descarga de Software”
179	Prueba Antivirus Antes de Usar en Sistemas de Empresa X	8.03.01.05	“Exploración del Software”
180	Prueba Antivirus en Máquina Independiente y Fuera de Ambiente de Producción	8.03.01.06	“Sistema de Prueba Antivirus”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
181	Todo Software y Archivos Ejecutables Salientes Deben Estar Libres de Virus	8.03.01.07	“Software y Ejecutables Salientes”
182	Antivirus en Cortafuegos, Servidores y Máquinas de Escritorio	8.03.01.08	“Instalación de Software Antivirus”
183	Al Menos Dos Paquetes Antivirus Deben Emplearse	8.03.01.09	“Múltiples Paquetes Antivirus”
184	Calcomanía Antivirus Obligatoria en Todos los Discos Provenientes del Exterior	8.03.01.10	“Calcomanía de Certificación Antivirus”
185	Proceso Obligatorio de Revisión de Software Descargado de Internet	8.03.01.11	“Exploración de Software Descargado”
186	Programas de Verificación de la Integridad del Sistema Obligatorios para Computadores Personales	8.03.01.12	“Verificación de la Integridad del Sistema”
187	Programas Antivirus Autorizados Obligatorios en PCs y Servidores LAN	8.03.01.13	“Programas Antivirus”
188	Software Antivirus Actual Obligatorio para Ciertos Computadores de Trabajadores	8.03.01.14	“Software Antivirus Actual”
189	Material Debe Estar Descifrado Antes de Verificar Virus	8.03.01.15	“Descifrado de Archivos para Verificar Virus”
190	Protección Contra Escritura Para Software en Micros y Estaciones de Trabajo	8.03.01.16	“Protección Contra Escritura para Software”
191	Copias de Respaldo Iniciales del Software de Microcomputadores	8.04.01.01	“Copias Maestras del Software”
192	Prueba del Software e Información Antes de Distribuir a Terceros	10.05.01.01	“Prueba e Información del Software”
193	Prohibición de Programas que Consuman Recursos Excesivos del Sistema	10.05.01.02	“Consumo de Recursos por Programas”
194	Toda Asociación con Virus Queda Prohibida	8.03.01.18	“Asociación con Virus Informáticos”
195	Identificación de requisitos de Seguridad Antes de Desarrollar/Adquirir	10.01.01.01	“Identificación de Requisitos de Seguridad”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
196	Desarrolladores Incluyen Seguridad en Sistemas Si Existe Solución Comercial	10.01.01.03	“Inclusión de Seguridad en Sistemas”
197	Cumplimiento de Convenciones en Desarrollo de Sistemas Organizacionales	10.05.01.03	“Convenciones en Desarrollo de Sistemas”
198	Prueba de Software con Datos Desclasificados En Lugar de Información de Producción	10.04.02.01	“Información Usada en Pruebas de Software”
199	Software Interno --Aviso de Falla en Operación	10.02.02.02	“Falla de Operación del Software”
200	Software Interno--Aviso de No Acción Tomada	10.02.02.03	“Retroalimentación del Software al Usuario”
201	Especificaciones Formales Obligatorias para el Software Desarrollado Internamente	10.01.01.04	“Especificaciones para Software Desarrollado Internamente”
202	Eliminación de Todas las Vías de Acceso No Autorizadas en Software de Producción	10.05.01.04	“Vías de Acceso en Software de Production”
203	Uso de Herramientas y Técnicas de Desarrollo Maduras	10.01.01.06	“Herramientas y Técnicas de Desarrollo Maduras”
204	Uso de Herramientas y Lenguajes de Software con Atributos de Seguridad No Probados	10.05.04.01	“Uso de Herramientas y Lenguajes de Software”
205	Uso de Lenguajes de Programación de Alto Nivel	10.01.01.07	“Lenguajes de Programación de Alto Nivel”
206	Re-Usabilidad de Software Desarrollado Internamente	10.01.01.08	“Re-Usabilidad del Software”
207	Convenciones en Nombres para Archivos de Producción	5.02.02.04	“Convenciones en Nombres de Archivos”
208	Etiquetado Especial para Todas las Transacciones Distintas de Producción	5.02.02.05	“Transacciones Distintas a Producción”
209	Documentación Obligatoria para Todos los Sistemas Empresariales de Producción	8.02.02.02	“Documentación para Sistemas de Producción”
210	Funcionalidad Permisible de los Sistemas Desarrollados Internamente	10.05.01.05	“Funcionalidad de los Sistemas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
211	Interrupción Inmediata de los Sistemas Si la Vida Está en Peligro	10.02.02.04	“ Interrupción del Sistema por Seguridad ”
212	Uso Restringido de Hardware y Software de Diagnóstico	9.05.05.05	“ Hardware y Software de Diagnóstico ”
213	Utilidades del Sistema Residentes en Medios de Almacenamiento de Producción	9.05.05.06	“ Almacenamiento de Utilidades del Sistema ”
214	Uso Restringido y Monitoreo de las Utilidades del Sistema	9.05.05.07	“ Uso de las Utilidades del Software del Sistema ”
215	Interfaces a Redes Externas Deben Ser Aprobadas por Seguridad Informática	8.05.01.03	“ Interfaces a Redes Externas ”
216	Acceso a Información Empresarial de Producción para Pruebas del Sistema	10.04.02.02	“ Acceso del Desarrollador a la Información de Producción ”
217	Separación Entre Ambientes de Producción y Desarrollo	8.01.05.01	“ Separación de Producción y Desarrollo ”
218	Separación Entre Ambientes de Programación y Pruebas	8.01.05.03	“ Separación de Programación y Pruebas ”
219	Acceso de Desarrolladores a Información de las Aplicaciones de Producción	9.06.01.13	“ Acceso a la Información de las Aplicaciones de Producción ”
220	Desarrolladores No Deben Realizar Pruebas Formales	8.01.05.04	“ Prueba del Software ”
221	Firma Especial Obligatoria Para Proyectos que Involucran Asuntos de Seguridad Humana	10.05.01.06	“ Proyectos que Involucran Seguridad Humana ”
222	Diseñadores y Desarrolladores Deben Notificar a Gerencia de Problemas Potenciales	10.05.01.07	“ Notificación de Problemas en los Sistemas ”
223	Quejas Sobre Errores y Problemas de Seguridad Ocasionados por Desarrolladores	10.02.02.05	“ Seguimiento de Errores y Problemas de Seguridad por Desarrolladores ”
224	Procedimiento Formal de Control de Cambios Obligatorio para Todos los Sistemas de Producción	10.05.01.08	“ Procedimiento de Control de Cambios ”
225	Cambios en el Sistema de Producción Deben Ser Consistentes con la Arquitectura de Seguridad	10.05.01.09	“ Consideraciones de Seguridad en Cambios en los Sistemas de Producción ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
226	Está Prohibida la Instalación por Usuario de Software en Computadores Personales	8.03.01.19.	“Instalación de Software por Usuario”
227	Prohibido que los Usuarios Actualicen Software para Computadores Personales	8.07.05.02	“Actualizaciones de Software de Computadores Personales”
228	Controles de Acceso Definidos Antes de Iniciar las Operaciones de Producción	10.05.01.10	“Controles de Acceso a las Operaciones de Producción”
229	Desactivar Identificadores de Usuarios Privilegiados Antes de Instalar Sistema Operativo	8.01.02.01	“Identificadores de Usuarios Privilegiados Suministrados por Proveedor”
230	Desactivar Características Innecesarias del Software Al Instalar	10.05.01.11	“Software Innecesario”
231	Remoción de Software Innecesario del Sistema Al Instalar	8.01.02.02	“Remoción de Software”
232	Cuando Preparar la Documentación de Cambios en los Sistemas de Producción	10.05.01.12	“Documentación de Cambios en Sistemas de Producción”
233	Documentación de Adiestramiento y Operación Requerida para Sistemas de Producción	10.05.01.13	“Documentación de Adiestramiento y Operaciones”
234	Carga de Programas Externos en Computadores Conectados a la Red	8.03.01.20	“Carga de Programas Externos”
235	Uso de Actualizaciones Automáticas para Software Requiere Autorización	8.03.01.21	“Actualizaciones Automáticas de Software”
236	Prueba de Software Externo Antes de su Uso	10.05.01.14	“Prueba de Software Externo”
237	Software Gratuito No Puede Utilizarse en Aplicaciones de Producción	12.01.02.01	“Fuente de Desarrollo de Software”
238	Detección Automática de Programas de Aplicación de Usuarios Finales	8.07.05.03	“Programas de Aplicación de Usuarios Finales”
239	Lógica de Negocios Crítica No Debe Residir en Computadores de Escritorio	8.07.05.04	“Lógica Crítica de Negocios”
240	Control del Movimiento de Software de Desarrollo a Producción	10.04.01.02	“Migración de Software”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
241	Software de Sistemas Proporcionado por Proveedores Debe Pasar por Control de Cambios	10.05.03.01	“Instalación de Software de Sistemas Proporcionado por Proveedores”
242	Revisión y Recompilación Requeridos Antes de Trasladar a Producción	10.05.01.15	“Revisión y Recompilación de Software”
243	Proceso Formal de Control de Cambios Requerido Para Aplicaciones del Negocio	10.05.01.16	“Proceso de Control de Cambios para Aplicaciones de Negocios”
244	Aprobación Separada Requerida para Controles del Sistema de Producción	8.02.02.04	“Controles de Sistemas de Producción”
245	Aprobación Requerida para Aplicaciones Multiusuario de Producción	8.02.02.05	“Aceptación de Aplicaciones de Producción”
246	Aprobación de Esfuerzos de Usuarios Finales en Desarrollo de Sistemas de Producción	8.02.02.06	“Desarrollo de Sistemas por Usuarios Finales”
247	Autorización Requerida para Cambios de Sistemas Operativos de Producción	8.01.02.03	“Cambios del Sistema Operativo de Producción”
248	Revisión Periódica de los Cambios al Sistema Operativo de Producción	8.01.02.04	“Revisiones de los Cambios al Sistema Operativo de Producción”
249	Prohibición de Trampas para Burlar Controles de Acceso	9.01.01.10	“Burlado de los Controles de Acceso”
250	Pronta Implementación de Software de Arreglo de Problema de Seguridad, Comandos, Etc.	8.01.03.01	“Arreglos de Seguridad”
251	Software de Sistemas y de Aplicaciones a Niveles Estables Más Recientes	8.01.02.05	“Versiones de Software”
252	Autorización Especial Requerida para Cambios en Paquetes de Software de Producción	10.05.01.17	“Autorización para Cambiar Paquete de Software de Producción”
253	Manenimiento del Software con Código Fuente en Lugar de Código Objeto	10.05.01.18	“Mantenimiento de Software”
254	Cronograma de Cambios en los Sistemas Informáticos de Producción de la Empresa X	10.05.01.20	“Implantación de Cambios en Sistemas Informáticos de Producción”
255	Regreso Rápido a Versiones Previas del Software de Producción	8.01.02.06	“Procedimientos de Retorno”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
256	Planes de Contingencia en la Conversión del Software de Producción	8.02.02.07	“ Planes de Contingencia en Conversión de Software ”
257	Cuándo se Requieren los Enunciados del Impacto de la Seguridad Informática	8.02.02.08	“ Análisis del Impacto sobre la Seguridad Informática ”
258	Enunciados del Impacto de la Seguridad para Aplicaciones del Negocio Nuevas o Modificadas	8.02.02.09	“ Enunciados Sobre el Impacto de la Seguridad ”
259	Enunciados de Integridad Escritos por el Proveedor	10.05.04.02	“ Enunciados de la Integridad del Software ”
260	Software Empacado y Desactivación Unilateral por Proveedor Tercero	10.05.03.02	“ Acceso de Proveedor Tercero a Software Empacado ”
261	Garantía Especial para Software Utilizado en Actividades Críticas del Negocio	12.01.02.03	“ Garantía Especial de Software ”
262	Software En Garantía Especial Debe Ser Verificado por Terceros	12.01.02.04	“ Verificación de Software En Garantía Especial ”
263	Formulario de Empresa X para Software Distribuido a Terceros	8.07.01.01	“ Software Distribuido a Terceros ”
264	Convenios con Terceros sobre el Uso de Software de Empresa X	8.07.01.02	“ Convenios de Software con Terceros ”
265	Entrega de Documentación de Sistemas a Terceros	8.06.04.01	“ Entrega de Documentación de Sistemas ”
266	Características y Funciones del Software Deben Revelarse por Completo en Documentación	10.05.01.21	“ Documentación de Características y Funciones del Software ”
267	Acceso a Papelerías, Chequeras y Otros Formularios de Empresa X	8.06.03.01	“ Acceso a Formularios ”
268	Fumar, Comer y Beber en la Sala de Computación	7.02.01.01	“ Fumar, Comer y Beber ”
269	Sistemas de Computación de Producción Debe Estar Físicamente Ubicados en Centro de Datos	7.02.01.02	“ Ubicación de Sistemas de Computación de Producción ”
270	Registros de Operador de Computadores Requeridos para Sistemas de Producción Multiusuario	8.04.02.01	“ Registros de Operadores de Computadores ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
271	Registros de Operador de Computadores Deben Ser Revisados Periódicamente	8.04.02.02	“Revisión de Registros de Operadores de Computadores”
272	Información Como Importante Activo de la Empresa X	3.01.01.03	“Manejo, Acceso y Uso de la Información”
273	Asignación de Derechos de Patente, Derechos de Autor y Otros Derechos de Propiedad Intelectual	6.01.04.01	“Derechos de Propiedad Intelectual”
274	Derechos de Propiedad sobre Programas de Computación y Documentación	6.01.03.01	“Derechos de Propiedad”
275	Propiedad Legal de Archivos y Mensajes en Sistemas Informáticos	5.02.01.01	“Propiedad de Archivos y Mensajes”
276	Recuperación de Propiedad Informática de la Empresa X	6.01.04.02	“Recuperación de la Propiedad de la Organización”
277	Atribución de Fuentes de Información	12.01.02.05	“Atribución de la Información”
278	Etiquetado de los Derechos de Paternidad a la propiedad Intelectual	12.01.02.06	“Etiquetado de la Propiedad Intelectual”
279	Avisos de Derechos de Autor en Programas de Computación y Documentación	12.01.02.07	“Avisos de Derechos de Autor en Software”
280	Trabajadores Pueden Hacer Múltiples Copias Sólo Si Es Razonable y Costumbre	12.01.02.08	“Copias Múltiples de la Información”
281	Revisión Periódica de los Convenios de Licencia del Software	12.01.02.09	“Revisión de los Convenios de Licencia del Software”
282	Adquisición de Sistemas y Evidencia de Licencias de Software	12.01.02.10	“Evidencia de Licencia de Software”
283	Registro de Productos de Sistemas de Información con Proveedores	7.02.04.01	“Productos de Sistemas Informáticos”
284	Pedido de Copias Autorizadas de Software Necesarias para Actividades Empresariales	12.01.02.11	“Copias Autorizadas de Software”
285	Cuándo es Permisible Hacer Copias Adicionales de Software	12.01.02.12	“Copias de Software”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
286	Remoción de Información y Software No Autorizados	12.01.02.13	“ Información y Software No Autorizados ”
287	Protección Aplicable del Derecho de Autor para la Información Enviada a Internet	12.01.02.14	“ Protección Aplicable del Derecho de Autor ”
288	Prohibido Copiar, Transferir o Divulgar Software	12.01.02.15	“ Duplicación de Software ”
289	Responsabilidad de Hacer Copias No Autorizadas de Software y Datos	12.01.02.16	“ Copias No Autorizadas de Software y Datos ”
290	Prohibidas Herramientas Utilizadas para Inhabilitar Seguridad de Sistemas	12.01.05.13	“ Herramientas de Prueba de la Seguridad del Sistema ”
291	Participación en Foros y Otros Sitios Piratas en Internet	12.01.02.17	“ Material Con Derechos de Autor No Autorizado ”
292	Manejo de Información Confidencial de Terceros	9.06.01.14	“ Información Confidencial de Terceros ”
293	Uso de la Información de la Empresa X para Propósitos No Empresariales	12.01.05.14	“ Uso Distinto al Empresarial de la Información de la Organización ”
294	Transferencia de la Información de la Empresa X a Terceros	4.02.02.02	“ Transferencia de Información a Terceros ”
295	Intercambios de Software O Datos con Terceros Requieren de Convenios	8.07.01.03	“ Convenios de Intercambio de Software y Datos ”
296	Designación del Software y los Sistemas Como Información Competitiva	5.01.01.01	“ Clasificación del Software y los Sistemas ”
297	Monitoreo de Internet Sobre Uso de Marcas Registradas y Materiales Con Derechos de Autor	12.01.02.19	“ Monitoreo en Internet del Uso de la Información ”
298	Uso en Internet de Otras Marcas Registradas y de Servicio de la Organización	12.01.02.20	“ Uso de Marcas Registradas de Terceros ”
299	Prohibición del Uso del Nombre de la Empresa X por Terceros	4.02.02.03	“ Uso por Parte de Terceros del Nombre de la Organización ”
300	Todo Uso Público Escrito del Nombre de la Empresa X Requiere Autorizaciónl	8.07.06.01	“ Uso del Nombre de la Organización ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
301	Pérdida de Conocimiento Crítico y Empleados Que Vuelan en Mismo Avión	6.01.04.03	“Empleados Que Viajan Conjuntamente”
302	Derecho de la Gerencia a Examiar los Datos Almacenados en los Sistemas de la Empresa X	12.01.05.15	“Examen de los Datos Almacenados en los Sistemas”
303	Pretextos Utilizados para Probar Servicio al Cliente y Políticas de Seguridad	4.01.07.01	“Uso de Investigadores”
304	Areas Donde Puede Usarse Monitoreo Electrónico de los Trabajadores	12.01.05.16	“Areas de Monitoreo Electrónico”
305	Divulgación de Información sobre Sistemas de Empresa X a las Autoridades	12.01.07.03	“Divulgación de Información a las Autoridades”
306	Derechos de Privacidad Renunciados al Cobrar Facturas u Obligar al Cumplimiento de Contratos	12.01.04.03	“Renuncia a Derechos de Privacidad”
307	Divulgación de Información Privada sin el Consentimiento de los Sujetos Data	12.01.04.04	“Divulgación de Información Privada”
308	Individuos Afectados por Cambios Materiales en Política de Privacidad Deben Ser Notificados	12.01.04.87	“Aviso de Cambio en Política de Privacidad”
309	Cambios en Política de Privacidad Requieren Resumen de Diferencias	12.01.04.88	“Resumen de Diferencias en Políticas de Privacidad”
310	Política de Privacidad Se Relaciona con Todo Tipo de Interacción con los Clientes	12.01.04.89	“Importancia de la Política de Privacidad”
311	Información Que Se Permite Recolectar Acerca de Empleados Potenciales	6.01.02.01	“Información de Empleado Potencial”
312	Prohibida Recopilación de Información Privada Excepto con Permiso	12.01.04.05	“Recopilación de Información Privada”
313	Información Personal Necesaria para el Funcionamiento Correcto del Negocio	12.01.04.06	“Información Personal para el Funcionamiento del Negocio”
314	Recopilación de Información Acerca de las Expresiones de los Derechos de la Primera Enmienda	12.01.04.07	“Información Sobre Libertad de Expresión”
315	Neceesidad de Recopilar Información Privada Debe Ser Justificada Primero	12.01.04.08	“Autorización de Recopilación de Información Privada”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
316	Recopilación de Datos Privados Sólo Si Es Legal y Necesario	12.01.04.09	“Recopilación de Datos Privados”
317	Prohibida la Recopilación Furtiva de Datos Privados de Clientes	12.01.04.10	“Recopilación Furtiva de Información Privada”
318	Recopilación de Información Personalmente Identificable Requiere de Aviso	12.01.04.12	“Aviso de Recopilación de Información”
319	Recopilación de Información Personal de Menores Requiere Permiso de los Padres	12.01.04.13	“Recopilación de Información Personal de Menores”
320	Recopilación de Información Personal Permisible Pero Se Prohibe la Distribución	12.01.04.14	“Distribución de la Información Personal”
321	Información de los Clientes Permisible de Recopilar	12.01.04.15	“Recopilación de Información de Clientes”
322	Métodos Menos Intrusivos Disponibles para Obtener Información Privada	12.01.04.16	“Métodos de Recopilación de Información Privada”
323	Prohibida la Captura Involuntaria de Información Personal Biométrica	12.01.04.17	“Captura de Información Biométrica”
324	Prohibida la Transferencia de Datos Personales Biométricos a Terceros	12.01.04.18	“Transferencia de Información Biométrica”
325	Puntos de Recopilación de Datos Personales y Política de Privacidad	12.01.04.90	“Puntos de Recopilación de Datos Personales y la Privacidad”
326	Debe Divulgarse Nombre de la Organización Que Recopila la Información Privada	12.01.04.91	“Identidad del Recolector de Información Privada”
327	Se Requiere Explicación de Por Qué Se Recopila Información Privada	12.01.04.92	“Explicación del Requerimiento de Información Privada”
328	Información Sobre el Monitoreo del Desempeño e Importancia en el Trabajo	12.01.07.04	“Información Sobre el Monitoreo del Desempeño”
329	Expectativas de Privacidad e Información Almacenada en los Sistemas de la Empresa X	12.01.04.19	“Expectativas de Privacidad e Información Almacenada en Sistemas de la Organización”
330	Se Requiere Permiso de Empleado Antes de Usar Monitoreo	12.01.07.05	“Permiso para Monitoreo”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
331	No Se Permite el Monitoreo de las Comunicaciones de los Empleados	12.01.07.06	“Monitoreo de las Comunicaciones de los Empleados”
332	Atención Gerencial a la Conducta de los Empleados Fuera de la Oficina	12.01.04.20	“Conducta de los Empleados Fuera de la Oficina”
333	Notificación de Sistemas Actuales de Monitoreo	9.07.02.13	“Herramientas de Monitoreo de Sistemas”
334	Todo Monitoreo de Usuario Debe Informarse al Gerente del Usuario y Registrarse	9.07.02.14	“Notificación y Registro de Monitoreo de Usuarios”
335	Gerentes Reciben Registros y Determinan Uso Apropriado de Internet	9.07.02.15	“Registros de Uso de Internet”
336	No Se Compilarán Perfiles de Uso de Internet por Clientes	9.07.02.16	“Perfiles de Uso de Internet por Clientes”
337	Monitoreo o Grabación de Conversaciones Telefónicas	12.01.07.07	“Monitoreo o Grabación de Conversaciones Telefónicas”
338	Monitoreo en Grupo en Lugar de Monitoreo Individual	9.07.02.17	“Monitoreo del Desempeño”
339	Actividades Anónimas de Monitoreo y Grabación	9.07.02.18	“Actividad de Monitoreo y Grabación”
340	Cronograma de Notificación Acerca del Monitoreo Electrónico del Desempeño	9.07.02.19	“Notificación de Monitoreo Electrónico del Desempeño”
341	Existencia de Sistemas Secretos Que Contengan Registros de Personal	12.01.04.21	“Sistemas Secretos”
342	Acceso Garantizado a la Información Personal Contenida en los Registros de la Empresa X	12.01.04.22	“Acceso a la Información Personal”
343	Distribución Periódica de los Registros del Personal Empleado	6.01.04.06	“Distribución de los Registros del Personal”
344	Empleados Potenciales Reciben Oportunidad para Rechazar Verificaciones de Crédito	6.01.02.02	“Verificaciones de Historia Crediticia de Empleados Potenciales”
345	Divulgación de Información Privada a Terceros	12.01.04.23	“Divulgación de Información Privada a Terceros”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
346	Transferencia de Datos Privados Sólo a Organizaciones con Suficientes Controles	12.01.04.24	“Transferencia de Datos Privados”
347	Registros de Terceros Que Reciben Información Privada	12.01.04.25	“Registros de Divulgación de Información Privada — Detalles”
348	Transferencia de Información Privada a Otros Países Requiere Autorización	12.01.04.26	“Transferencia Internacional de Información Privada”
349	Individuos Reciben Oportunidad de Bloquear Divulgación de Información Privada	12.01.04.27	“Bloqueo de Divulgación de Información Privada”
350	Divulgación de Nombres, Cargos y Otra Información de Trabajadores	12.01.04.28	“Divulgación de Información de Contacto de Trabajadores”
351	Divulgación de Razón para Cesar Empleado	12.01.04.29	“Divulgación de Razón de Cese de Relación Laboral”
352	Divulgación de Información de Cambio en Situación del Trabajador	12.01.04.30	“Divulgación de Cambio de Situación”
353	Otorgar a Trabajadores Acceso a la Divulgación de los Registros de los Datos Privados	12.01.04.31	“Acceso a Divulgación de Registros de Datos Privados”
354	Privacidad de la Información del Desempeño Individual del Trabajador	12.01.04.32	“Información Sobre Desempeño del Trabajador”
355	Confidencialidad de la Información de Investigaciones Internas	12.01.07.08	“Confidencialidad de la Información de las Investigaciones Internas”
356	Divulgación Obligatoria de la Información de Salud y Seguridad de los Trabajadores	6.01.04.07	“Información Sobre Salud y Seguridad”
357	Uso de Pruebas para Determinar Información sobre Estilo de Vida, Política y Religión	6.01.02.03	“Información Sobre Estilo de Vida del Empleado Potencial”
358	Privacidad de Archivos Personales Almacenados en Computadores y en Escritorios	12.01.04.33	“Privacidad del Archivo Personal”
359	Mantenimiento de Registros de Información Privada Divulgada a Terceros	12.01.04.34	“Registros de Divulgación de Información Privada — Mantenimiento”
360	Protección de la Privacidad de la Información del Cliente	12.01.04.35	“Privacidad de la Información del Cliente”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
361	Divulgación de la Información del Cliente Que Incluye Identidad del Cliente	12.01.04.38	“Divulgación de la Información del Cliente”
362	Derecho del Cliente a Saber Cuáles Terceros Reciben Sus Datos	12.01.04.40	“Divulgación de Receptor de Información del Cliente”
363	Oportunidad del Cliente para Objectar Solicitudes de Sus Registros	12.01.04.41	“Notificación al Cliente de Solicitudes de Registros”
364	Política de Privacidad Se Considera Contrato Realizado al Momento de Proporcionar Información	12.01.04.42	“Aplicación de Política de Privacidad”
365	Privacidad de Direcciones de Correo Electrónico y Números Telefónicos de Remitentes	12.01.04.43	“Privacidad de Información de Contacto de Remitentes”
366	Divulgacion Telefónica Requiere de Identificación Positiva	8.07.07.02	“Divulgación Telefónica de Información”
367	No Puede Haber Discusiones de Información Privada en Sitios Públicos	8.07.07.03	“Discusiones En Sitios Públicos”
368	Solicitud de Anonimato del Cliente en Sistemas de Empresa X	12.01.04.44	“Anonimato del Cliente”
369	Reconocimiento o Referencia Pública de Clientes Famosos	12.01.04.45	“Identificación de Clientes Famosos”
370	Distribución de Información Estadística Acerca de los Registros de los Clientes	12.01.04.46	“Información Estadística de los Registros de los Clientes”
371	Divulgación de Registros Computarizados Que Reflejen Actividades del Cliente	12.01.04.47	“Divulgación del Registro de las Actividades del Cliente”
372	Eliminación de Información Registrada Acerca de las Actividades del Cliente	12.01.03.01	“Información de Registro del Cliente”
373	Monitoreo de Mensajes de Correo Electrónico	9.07.02.20	“Monitoreo de Mensajes de Correo Electrónico”
374	Derecho del Trabajador a Leer Mensajes Electrónicos de Terceros	8.07.04.01	“Revisión de Mensajes de Correo Electrónico de Terceros”
375	Cumplimiento del Empleado de la Política de Privacidad de la Empresa X	12.01.04.48	“Cumplimiento de la Privacidad”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
376	Se Requiere Consentimiento para Acciones Cuestionables en los Sistemas	12.01.04.49	“Consentimiento para Acciones Cuestionables en los Sistemas”
377	Creadores de Registros Deciden Si Sujetos Pueden Ver Registros	12.01.04.50	“Autorización de Acceso a los Registros Individuales”
378	Divulgación de Usos Propuestos de la Información Personal Antes de su Recopilación	12.01.04.51	“Divulgación de Usos Propuestos de Información Personal”
379	Clientes Reciben Oportunidad de Decidir Recibir Correo Directo	8.07.07.04	“Clientes Rechazan Correo Directo No Solicitado”
380	Colocación de la Publicidad en Internet con Firmas que Valoren la Privacidad	8.07.06.02	“Publicidad en Internet”
381	Copias de Información Que Aparece en el Archivo de Personal Propio	12.01.04.52	“Acceso al Archivo del Personal”
382	Condiciones Bajo las Cuales los Empleados Pueden Examinar Sus Archivos	12.01.04.53	“Revisión del Archivo del Empleado”
383	Derecho del Empleado a Agregar Enunciado Explicativo al Archivo de Personal	12.01.04.54	“Declaración Explicativa del Empleado”
384	Información Supuestamente Incorrecta A Corregirse o Etiquetarse como Disputable	12.01.04.55	“Información Personal Incorrecta”
385	Esfuerzos Requeridos Para Garantizar la Integridad de Todos los Registros Personales	12.01.04.56	“Integridad del Registro Personal”
386	Procedimientos Documentados Requeridos para las Actividades de Manejo del Registro Personal	12.01.04.57	“Manejo del Registro Personal”
387	Esfuerzos Requeridos para Garantizar que los Registros Personales Se Utilizan Solamente de la Manera Debida	12.01.04.58	“Uso del Registro Personal”
388	Uso de la Información Personal para Nuevos Propósitos	12.01.04.60	“Uso de la Información Personal para Nuevos Propósitos”
389	Enlace de Información Anónima con Información Identificable por Persona	12.01.04.61	“Enlace de Información Anónima”
390	Uso y Divulgación de Información Personal Acerca de los Clientes	12.01.04.62	“Información Personal de los Clientes”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
391	Derecho del Cliente a Conocer Naturaleza de la Información Personal	12.01.04.63	“Acceso del Cliente a Información Personal”
392	Reventa o Diseminación Posterior de la Información de Contacto del Cliente	12.01.04.64	“Uso de la Información de Contacto del Cliente”
393	Distribución de Materiales de Mercadeo No Solicitados de la Empresa X	8.06.03.02	“Distribución de Materiales de Mercadeo”
394	Cambios Importantes en los Sistemas y Comité de Revisión del Impacto Sobre la Privacidad	8.02.02.10	“Revisión del Impacto Sobre la Privacidad”
395	Deben Revelarse Fuente y Propósito de Cookies	8.07.06.03	“Cookies en Internet”
396	Se Requiere de Necesidad Real Antes de Usar Cookies	8.05.01.06	“Cookies”
397	No Debe Haber Identificadores Personales Secretos o Números de Serial Incluidos	12.01.04.65	“Información Personal Incluida”
398	No Deben Aparecer Identificadores Personales en Ubicaciones Accesibles Públicamente	12.01.04.66	“Identificadores Personales en Ubicaciones Públicas”
399	Corte del Enlace Entre la Información Identificadora y los Datos de Investigación	12.01.04.68	“Enlaces Entre la Información Privada y la Identificadora”
400	No Debe Haber Enlaces Entre la Información Privada y Otros Tipos de Información	12.01.04.69	“Enlaces con Información Privada”
401	Retención de Información Personal Sólo Mientras Se Necesite para el Negocio	12.01.03.02	“Retención de la Información Personal”
402	Destrucción Rutinaria de los Registros de Transacciones Evita Compilación de Perfiles	12.01.03.03	“Destrucción de Registros de Transacciones”
403	Individuos Reciben Oportunidad de Rechazar Participación en Sistemas de Datos Privados	12.01.04.70	“Opción de Participación en Sistema de Datos Privados”
404	Todas las Comunicaciones de Mercadeo Deben Proporcionar Oportunidad de Rechazo	8.07.03.03	“Posibilidad de Rechazo de Comunicación de Mercadeo”
405	Individuos Deben Escoger Para Ser Incluidos en Sistemas Que Manejen Datos Privados	12.01.04.72	“Autorización para Inclusión en Sistemas de Datos Privados”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
406	Acción Inmediata para Individuos Que Soliciten su Remoción de la Base de Datos	12.01.04.75	“Remoción de Individuos de la Base de Datos”
407	Individuos Pueden Bloquear el Uso de Sus Datos Privados	12.01.04.77	“Bloqueo del Uso de Datos Privados”
408	Individuos Deben Autorizar Nuevos Usos de Datos Personales Despues de una Fusión o Adquisición	12.01.04.81	“Usos de Datos Personales Despues de Una Fusión o Adquisición”
409	Cambios de la Estructura del Negocio No Permiten la Transferencia de los Datos Privados	12.01.04.82	“Cambios en la Estructura del Negocio y la Transferencia de Datos Privados”
410	Mantenimiento de Indice de Bases de Datos Que Contengan Información Privada	12.01.04.83	“Indices de Base de Datos Que Contienen Información Privada”
411	Denegación de Beneficios Debido a la Negativa de Proporcionar Información Innecesaria	12.01.04.85	“Negativa a Proporcionar Información Innecesaria”
412	Acuerdos de Confidencialidad Requeridos para Todos los Trabajadores de la Empresa X	6.01.03.02	“Acuerdos de Confidencialidad — Organización”
413	Compromiso en Acuerdos de Confidencialidad Requerido para la Información Privada y Confidencial	4.02.02.06	“Compromiso en Acuerdos de Confidencialidad”
414	Acuerdos de Confidencialidad Requeridos para Todo el Personal de Reparación de Máquinas de Oficina	4.02.01.05	“Acuerdo de Confidencialidad para el Personal de Reparación de Máquinas de Oficina”
415	Cambios en el Empleo Requieren Revisión de los Acuerdos de Confidencialidad	6.01.03.03	“Cambios en el Empleo”
416	Restricciones Predeterminadas Sobre la Diseminación de la Información de la Empresa X	4.02.01.06	“Diseminación de la Información”
417	Notificación de Sospechas en Pérdida o Divulgación de Información Confidencial	6.03.01.01	“Pérdida o Divulgación de Información Sensible”
418	Divulgación de Detalles Técnicos de Sistemas Informáticos a Solicitantes de Empleo	6.01.02.04	“Divulgación de Información a Solicitantes de Empleo”
419	Divulgación de Especificidades del Control de los Sistemas Informáticos a Terceros	8.06.03.03	“Divulgación de los Controles del Sistema Informático”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
420	Divulgación de Información Financiera a Ciertos Individuos	8.07.07.05	“Divulgación de Información Financiera”
421	Divulgación de Información Acerca de las Vulnerabilidades del Sistema Informático	6.03.01.02	“Divulgación de las Vulnerabilidades del Sistema Informático”
422	Información en Detalle de la Vulnerabilidad en Notas de Prensa Debe Ser Baja	6.03.01.03	“Notas de Prensa Sobre Información de Vulnerabilidad”
423	Divulgación de la Explotación de la Vulnerabilidad del Sistema y Datos de la Víctima	6.03.01.04	“Explotación de la Vulnerabilidad del Sistema y Datos de la Víctima”
424	Divulgación del Código Fuente del Software de Penetración de Sistemas y su Análisis	12.03.02.01	“Código Fuente del Software de Penetración de Sistemas”
425	Mecanismos de Seguridad No Deben Ser Comprometidos por los Clientes	9.01.01.11	“Comprometer Mecanismos de Seguridad para los Clientes”
426	Presentación de Imagen de Bajo Perfil y Segura	8.07.06.04	“Presentación de la Imagen Pública”
427	Sistemas de Control de Acceso a la Información y la Teoría del Mosaico	9.01.01.12	“Restricciones a la Recopilación de la Información”
428	Limitaciones a la Recopilación de Precios por Terceros	4.02.02.08	“Recopilación de Información de Precios por Terceros”
429	Prevención de Robo de Identidad Mediante la Restricción del Acceso a la Información Personal	9.06.01.15	“Acceso a la Información Personal”
430	Acceso al Almacén de Datos Restringido a Gerencia Media y Alta	9.06.01.16	“Acceso al Almacén de Datos”
431	Vacilación para Esconder Verdadera Naturaleza de la Señal	8.05.01.07	“Esconder Transmisión de la Información”
432	Derecho a Bloquear, Esconder, Denegar o Descontinuar Servicio en Cualquier Momento	9.04.01.01	“Descontinuación del Servicio”
433	Información Con Múltiples Clasificaciones de Confidencialidad en Un Solo Sistema	5.02.01.13	“Sistemas de Computación con Múltiples Clasificaciones de Sensibilidad”
434	Escogencia de Clasificaciones para Medios de Almacenamiento de Datos	5.02.01.14	“Clasificaciones de Medios de Almacenamiento de Datos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
435	Esquema de Clasificación de Datos en Cuatro Categorías	5.02.01.02	“Clasificación de Datos en Cuatro Categorías”
436	Esquema de Clasificación de Datos en Tres Categorías	5.02.01.03	“Clasificación de Datos en Tres Categorías”
437	Prefijos Descriptivos para las Categorías de Clasificación de Datos	5.02.01.06	“Prefijos de Categorías de Clasificación de Datos”
438	Secretos Empresariales Específicamente Identificados Antes de la Divulgación	5.02.02.06	“Divulgación de Secretos Industriales”
439	Los Secretos de la Empresa X Deben Estar Nombrados y Descritos en la Página de Intranet	8.07.06.05	“Secretos Industriales en la Intranet”
440	Jefe Legal Es el Unico Que Puede Declarar la Información Como Secreto Empresarial	5.02.01.07	“Declaración de Secreto Industrial”
441	Requerimientos del Sistema de Etiquetado de Clasificación Limitada de Datos	5.02.02.07	“Etiquetado de Clasificación de Datos”
442	Información Tratada como Secreto Cuando No Se Conoce la Etiqueta de Confidencialidad	5.02.02.08	“Etiqueta de Sensibilidad Desconocida”
443	Etiquetas de Clasificación de Datos Específicas por Departamento Permisibles	5.02.02.09	“Etiquetas de Clasificación por Departamento”
444	Responsabilidad de Asignar Etiquetas del Sistema de Clasificación de Datos	5.02.01.09	“Asignación de Etiquetas de Clasificación de Datos”
445	Responsabilidad de Etiquetar Información Externa	5.02.02.10	“Etiquetado de Información Externa”
446	Creador Debe Seleccionar Etiqueta de Clasificación de Datos para Nuevos Archivos y Mensajes	5.02.02.11	“Etiquetas de Clasificación Para Nueva Información”
447	Requerimientos Completos del Etiquetado del Sistema de Clasificación de Datos	5.02.02.12	“Etiquetado Completo de la Clasificación”
448	Ubicación de las Etiquetas de Sensibilidad en Papel	5.02.02.13	“Etiquetas de Sensibilidad en Papel”
449	Material Encuadrado y las Etiquetas de Confidencialidad	5.02.02.14	“Etiquetado de Material Impreso Encuadrado”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
450	Etiquetado y Presentación de Información Confidencial a los Usuarios de los Computadores	5.02.02.15	“Presentación de la Información Sensible”
451	Uso de Etiquetas en el Ciclo de Vida de la Información Confidencial	5.02.02.16	“Etiquetado Durante el Ciclo de Vida de la Información”
452	Mantener, Propagar y Reestablecer Etiquetas de Clasificación de Datos	5.02.02.17	“Mantenimiento de Etiquetas de Clasificación”
453	Etiquetas para Series de Información Con Distintas Confidencialidades	5.02.01.10	“Etiquetado de Clasificación Múltiple”
454	Nueva Etiqueta Después de la Exposición del Medio de Almacenamiento a Datos o Aplicaciones Secretos	5.02.01.11	“Exposición de Medios a Datos Secretos”
455	Las Etiquetas de Clasificación Generadas por Usuarios No Limitan a la Empresa X	5.02.01.12	“Etiquetas de Clasificación Generadas por Usuarios”
456	Permiso Requerido Para Hacer Copias de Información Sensible	5.02.02.18	“Copiado de Información Sensible”
457	Seguimiento de Copias de Información Sensible	5.02.02.19	“Seguimiento de Información Sensible”
458	Destrucción de Productos Intermedios Que Contengan Información Sensible	5.02.02.20	“Productos Intermedios Con Información Sensible”
459	Destrucción de Copias Sobrantes de Información Sensible	5.02.02.21	“Copias Sobrantes de Información Sensible”
460	Obligatorio Atender Operación Cuando se Imprime Información Sensible	5.02.02.22	“Impresión de Información Sensible”
461	Numeración de Páginas y Responsabilidad por Información Sensible	5.02.02.23	“Responsabilidad por la Información Sensible”
462	Acuerdos de Confidencialidad con Terceros y la Información Confidencial	4.02.01.07	“Acuerdos de Confidencialidad — Terceros”
463	Divulgación de Información de Terceros en Manos de la Empresa X	9.01.01.13	“Divulgación de la Información de Terceros”
464	Información Privada y Confidencial Enviada por Correo Interno o Externo	8.07.05.05	“Envío de Información Privada y Confidencial”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
465	Información Secreta Enviada por Correo Interno o Externo	8.07.07.06	“Envío de Información Secreta”
466	Obligatorio Dos Sobres para la Información Sensible Enviada por Correo	8.07.07.07	“Envío de Información Sensible”
467	Métodos Permisibles para la Transmisión de Información Secreta en Papel	8.07.07.08	“Transmisión de Información Secreta en Papel”
468	Papel Especial para Evitar Copiado de Documentos Confidenciales	5.02.02.24	“Prevención del Copiado de Documentos Sensibles”
469	Información Secreta Sólo Puede Imprimirse en Papel Que Indique Originales	5.02.02.25	“Impresión de Información Secreta”
470	Entrega de Salidas Confidenciales de Computadores al Receptor Correspondiente	5.02.02.26	“Entrega de Salidas Computarizadas Confidenciales”
471	Entrega Via Courier de Información Confidencial	5.02.02.27	“Uso de Mensajeros”
472	Acuse de Recibo Obigatorio para Entregas de Información Secreta	5.02.02.28	“Entrega de Información Secreta”
473	Acuse de Recibo Inmediato por Información Secreta	5.02.02.29	“Recepción de Información Secreta”
474	Libro de Registros para Movimientos de Documentos Secretos	5.02.02.30	“Registro del Movimiento de Documentos Secretos”
475	Números Secuenciales para Documentos Secretos	5.02.02.31	“Números Secuenciales para Documentos Secretos”
476	Los Que Tengan Custodia de la Información Sensible Deben Restringir el Acceso	5.02.02.32	“Aseguramiento de la Información Sensible”
477	Aviso y Operación de Envío de Información Sensible Vía Fax	8.07.05.06	“Envío de Información Sensible Vía Fax — Notificación”
478	Envío de Información Sensible Vía Fax Requiere Presencia Humana	8.07.05.07	“Envío de Información Sensible Vía Fax — Presencia Humana”
479	Envío de Información Sensible Via Fax por Terceros No Confiables	8.07.05.08	“Envío de Información Sensible Vía Fax — Intermediarios”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
480	Acuse de Recibo de Hoja de Cubierta Antes de Enviar Información Sensible Vía Fax	8.07.05.09	“Envío de Información Sensible Vía Fax — Hoja de Cubierta”
481	Cuándo es Permisible Enviar Información Sensible Vía Fax	8.07.05.10	“Envío de Información Sensible Vía Fax — No Cifrada”
482	Seguridad Física en Destino para el Envío de Información Sensible Vía Fax	8.07.05.11	“Envío de Información Sensible Vía Fax — Seguridad Física”
483	Cifrado Requerido para Enviar Información Secreta Vía Fax	8.07.05.12	“Envío de Información Secreta Vía Fax — Cifrado”
484	Contraseña Requerida Para Enviar Información Secreta Vía Fax	8.07.05.14	“Envío de Información Secreta Vía Fax — Contraseñas”
485	Cubierta de Fax Debe Contener Aviso de Diseminación Restringida	8.07.05.15	“Aviso en Cubierta de Fax”
486	Firmas Legales Deben Enviarse por Medios Tradicionales de Papel	8.07.07.09	“Firmas Legales”
487	Discusión de Información Secreta y Uso de Altavoces Telefónicos	8.07.05.16	“Información Secreta en Altavoces Telefónicos”
488	Discusión Telefónica de Información Sensible	8.07.07.10	“Conversaciones Telefónicas Sobre Información Sensible”
489	Uso de Celulares o Inalámbricos para Discusiones Secretas	8.07.07.11	“Teléfonos Celulares o Inalámbricos”
490	Discusiones Secretas en Micrófonos Inalámbricos y Redes Radiales	8.07.07.12	“Transmisión Inalámbrica de Información Secreta”
491	Teléfonos de Internet No Deben Usarse para Discusiones Secretas	8.07.06.06	“Servicios Telefónicos en Internet”
492	Diseminación Secundaria de la Información Secreta	9.06.01.17	“Diseminación Secundaria de la Información Secreta”
493	Viajes en Transporte Público con Información Secreta	8.07.02.02	“Viajes con Información Secreta”
494	Exposición de Información Confidencial En Sitios Públicos	8.07.07.13	“Exposición Pública de Información Sensible”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
495	Discusiones de la Información Secreta En Areas Administrativas de la Empresa X	8.07.07.14	“Discusiones En Areas Administrativas”
496	Almacenamiento de Información Secreta en Computadores Portátiles	9.08.01.03	“Información Secreta en Computadores Portátiles”
497	Controles para Computadores Portátiles con Información Sensible	9.08.01.05	“Computadores Portátiles con Información Sensible”
498	Computadores Portátiles Deben Ser Equipaje de Mano en Aviones	9.08.01.06	“Computadores Portátiles en Aviones”
499	Información Secreta a un País Extranjero	8.07.02.03	“Transporte Internacional de Información Secreta — Seguridad”
500	Permiso Necesario para Llevar Información Secreta a País Extranjero	8.07.02.04	“Transporte Internacional de Información Secreta — Autorización”
501	Drivers de Cifrado para Discos Flexibles Evitan Divulgación	8.06.01.01	“Discos Flexibles”
502	Remoción de Información Sensible de las Instalaciones de la Empresa X	8.06.03.04	“Remoción de Información Sensible”
503	Información Secreta No Debe Salir de la Empresa X en Ninguna Forma	8.06.03.05	“Información Secreta Fuera de Oficinas”
504	Registro de Información Sensible Removida de Instalaciones de Empresa X	8.06.03.06	“Registro de Remoción de Información Sensible”
505	Manejo de Información Sensible en Papel Fuera de las Instalaciones de Empresa X	8.07.02.05	“Remoción de Información Sensible en Papel”
506	Transferencia de Información Sensible a Terceros en Medios Computarizados	8.07.02.06	“Transferencia de Información Sensible”
507	Certificado de Destrucción En Lugar de Retorno de Medios de Almacenamiento	8.07.01.04	“Certificado de Destrucción de Medios de Almacenamiento”
508	Confidencialidad de la Documentación Computarizada de la Empresa X	8.06.04.02	“Confidencialidad de la Documentación”
509	Información Secreta Enviada por Correo Electrónico	8.07.04.02	“Información Secreta en Correo Electrónico”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
510	Estaciones de Trabajo Sin Discos Deben Ser Utilizadas por Trabajadores del Departamento de Investigación y Desarrollo	8.07.05.17	“Estaciones de Trabajo Sin Discos”
511	Sistemas Informáticos No Aptos para Información Que Depende de un Espacio de Tiempo	8.07.05.18	“Información Sensible al Tiempo”
512	Uso de Discos Duros para Almacenar Información Sensible	8.07.05.19	“Almacenamiento de Información Sensible”
513	Mezcla de Información Confidencial y No Confidencial	8.06.01.02	“Almacenamiento de Información de Clasificación Mixta”
514	Escritorios y Areas de Trabajo Limpios	7.03.01.01	“Escritorios Limpios — Horas No Hábiles”
515	Política Tradicional de Escritorios Limpios	7.03.01.02	“Escritorios Limpios — Uso Activo”
516	Aseguramiento de Información Confidencial En Sitios Desatendidos	7.03.01.04	“Areas Desatendidas”
517	Almacenamiento de Información Sensible en Computadores Personales	9.08.01.07	“Información Sensible en Computadores Personales”
518	Almacenamiento de Información Sensible Cuando No Se Use	7.03.01.05	“Almacenamiento de Información Sensible”
519	Período de Retención Obligatorio para Toda Información Sensible	12.01.03.04	“Retención de la Información Sensible”
520	Fecha para Desclasificación Debe Ser Especificada Si Se Conoce	5.02.01.15	“Fecha de Desclasificación”
521	Desclasificación Acelerada y Degradación de la Información Confidencial	5.02.01.16	“Desclasificación Acelerada de la Información”
522	Extensión de la Fecha de Desclasificación o Degradación	5.02.01.17	“Prórroga para la Desclasificación”
523	Cronograma Automático para la Degradación de la Información de la Empresa X	5.02.01.18	“Cronograma de Desclasificación”
524	Revisión Anual de la Desclasificación de la Información Confidencial	5.02.01.19	“Revisión Anual de la Desclasificación”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
525	Desclasificación de la Información Sensible Requerido Tan Pronto Sea Práctico	5.02.01.20	“Desclasificación de la Información Sensible”
526	Destrucción/Almacenamiento de la Información Sensible Antes de Finalizar Servicio	5.02.02.34	“Medios de Almacenamiento de Información Sensible”
527	Liberación de Medios de Almacenamiento Antes de Limpieza Computarizada	8.06.03.07	“Liberación de Medios de Almacenamiento de Computación”
528	Destrucción de Información Confidencial en Medios de Almacenamiento	8.06.02.01	“Destrucción de Información Sensible”
529	Inicialización Obligatoria para Borrar Información Confidencial	8.06.01.03	“Borrado de Información Sensible”
530	Métodos Autorizados para Disponer de Información Confidencial en Papel	8.06.02.02	“Disposición de Información en Papel”
531	No Deben Utilizarse Máquinas Trituradoras de Papel en Tiras para la Destrucción de la Información Confidencial	8.06.02.03	“Máquinas Trituradoras de Papel en Tiras”
532	Areas Que Contengan Información Confidencial Deben Poseer Destructoras	8.06.03.08	“Areas Con Información Sensible”
533	Uso de Contenedores Seguros para Todas las Disposiciones Menos las de Información Secreta	8.06.02.04	“Contenedores Seguros de Información”
534	Equipo de Seguridad Debe Seguir Instrucciones para la Destrucción de la Información	8.06.02.05	“Instrucciones para la Destrucción de la Información”
535	La Destrucción de la Información Sensible Debe Seguir Procedimientos Especificados	8.06.02.06	“Procedimientos para la Destrucción de la Información Sensible”
536	Personas Autorizadas para Destruir Información Sensible de la Empresa X	8.06.02.07	“Personal para Destrucción de Información”
537	Uso de Cajas Metálicas para Guardar Información Sensible Mientras Se Destruye	8.06.02.08	“Cajas para la Destrucción de Información Sensible”
538	Destrucción de Materiales Usados en el Manejo de Información Sensible	8.06.02.09	“Materiales Usados con Información Sensible”
539	Autorización Requerida Antes de Acceder a Información Sensible o Valiosa	9.06.01.18	“Acceso a Información Sensible o Valiosa”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
540	Acceso a Información Secreta Otorgado Individualmente (No Grupalmente)	9.06.01.19	“Acceso a la Información Secreta”
541	Privilegios del Sistema Otorgados por Delegación de Autoridad	9.02.02.11	“Otorgamiento de Privilegios del Sistema”
542	Acuerdos de Confidencialidad y Divulgacion de la Información Confidencial	4.02.01.08	“Acuerdos de Confidencialidad”
543	Instrucciones Específicas de Manejo para los Receptores de Información Confidencial	4.02.02.09	“Manejo de Información Sensible”
544	Solicitudes de Información de Empresa X Enviadas a Relaciones Públicas	9.01.01.14	“Solicitudes de Información Organizacional”
545	Prohibición de Divulgar Proyectos de Clientes, Estrategias, Etc.	9.01.01.15	“Divulgación de Información de Negocios del Cliente”
546	Información de Mercadeo Nunca Debe Compartirse con Competidores	9.01.01.16	“Compartir Información de Mercadeo”
547	Información Liberada al Público Debe Tener Una Sola Fuente Oficial	9.01.01.17	“Información Liberada al Público — Nombre del Contacto”
548	Autorización Requerida Antes de Liberar Información de la Empresa X	9.01.01.19	“Liberación de Información de la Organización”
549	Representaciones Públicas Acerca de Futuras Ganancias o Productos	9.01.01.20	“Ganancias o Productos Futuros”
550	Período de Espera Antes de Divulgación Externa de la Información Solicitada	9.01.01.21	“Solicitudes Externas de Información”
551	Liberación por Fases al Público de Información Confidencial Controversial	9.01.01.22	“Información Sensible Controversial”
552	Autorización para Avisos de Empleos y Divulgación de Materiales Confidenciales	9.01.01.23	“Avisos Solicitando Empleados”
553	Procedimiento Establecido para Revisar Información Liberada al Público	9.01.01.24	“Información Liberada al Público — Autorización”
554	Revisión Previa de Discursos, Presentaciones, Papeles Técnicos, Etc.	9.01.01.25	“Comunicaciones Públicas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
555	Condiciones para la Aceptación de Información Confidencial de Terceros	4.02.02.10	“Recepción de Información de Terceros”
556	Firma de Acuerdos de Confidencialidad de Terceros sin Autorización	12.01.02.21	“Acuerdos de Confidencialidad de Terceros”
557	Acceso a la Información Confidencial para Trabajadores Temporales y Consultores	4.02.01.09	“Acceso para Trabajadores Temporales y Consultores”
558	Trabajadores Tienen Derecho a Conocer Todos los Peligros del Sitio de Trabajo	6.01.04.08	“Peligros Laborales”
559.	Naturaleza de las Etiquetas en Productos y Servicios Peligrosos	5.02.02.35	“Etiquetado de Productos y Servicios Peligrosos”
560	Evitar Presionar Antiguos Empleados de Competidores	6.01.03.04	“Acuerdos de Confidencialidad con Antiguos Patrones”
561	Divulgación de Políticas y Procedimientos de Seguridad Informática Relativos a la Privacidad	6.02.01.02	“Políticas y Procedimientos Relativos a la Privacidad”
562	Asistentes No Invitados a Reuniones Donde Se Discute Información Secreta	8.07.07.15	“Asistentes a Reuniones”
563	Reuniones con Terceros en Salones de Conferencia	8.07.07.16	“Reuniones con Terceros”
564	Divulgación Oral de Información Confidencial en Reuniones	8.07.07.17	“Información Confidencial en Reuniones”
565	Pizarrones Deben Borrarse Despues de Reuniones	8.07.07.18	“Superficies Borrables”
566	Borrado de Información Confidencial en Pizarrones	8.07.07.19	“Borrado de Superficies Borrables”
567	Naturaleza y Ubicación de la Información de la Empresa X Es Confidencial	9.01.01.27	“Naturaleza y Ubicación de la Información de la Organización”
568	Políticas y Procedimientos de Seguridad Informática Son para Uso Interno Solamente	3.01.01.11	“Uso de Políticas y Procedimientos de Seguridad Informática”
569	Ubicación de los Centros de Procesamiento de Datos Se Considera Confidencial	7.02.01.03	“Dirección de los Centros de Computación”
570	Prohibido Explorar en los Sistemas y Redes de la Empresa X	9.01.01.28	“Exploración de Sistemas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
571	Revisión Autorizada por el Administrador del Sistema de los Archivos Privados de los Usuarios	12.01.04.94	“Revisión de los Archivos Privados de Usuarios”
572	Apagado Obligatorio para los Sistemas Que Procesen Información Confidencial	7.03.01.06	“Apagado de Computadores”
573	Cubrir Información Sensible al Ser Interrumpido en el Trabajo	7.03.01.07	“Cubrir Información Sensible”
574	Nunca Prestar Computadores Que Contengan Información Sensible a Otros	9.08.01.08	“Préstamo de Computadores Que Contienen Información Sensible”
575	Todos los Trabajadores Deben Recibir y Usar Gabinetes con Llave	7.03.01.08	“Gabinetes de Archivo con Llave”
576	Fechas Prohibidas de Compra-Venta de Acciones para Empleados	6.01.04.09	“Transacciones Bursátiles de Empleados”
577	Máquinas de Dictado y Grabadores para Información Sensible	8.07.05.20	“Grabación de Información Sensible”
578	Limpieza Periódica para Evitar Dispositivos de Espionaje	7.01.03.01	“Limpieza Periódica para Evitar Equipos de Espionaje”
579	Meta Cuantitativa Específica para Disponibilidad del Sistema	8.01.01.04	“Disponibilidad del Sistema”
580	Limitación de la Capacidad del Usuario para Demorar o Interrumpir el Servicio	8.07.05.21	“Consumo Excesivo de Recursos”
581	Establecimiento y Uso de Facilidades para Inhabilitar Controles	9.05.05.08	“Facilidades para Inhabilitar Controles”
582	Definición Gerencial de las Circunstancias Para Usar la Inhabilitación de los Controles	9.05.05.09	“Uso de la Inhabilitación de los Controles”
583	Generación y Revisión de Registros que Muestren Uso de las Facilidades de Inhabilitación	9.07.02.21	“Registro de Inhabilitaciones”
584	Equipo Requerido para el Soporte del Ambiente Computacional	7.02.01.04	“Controles Ambientales del Centro de Computación”
585	Equipo de Protección Eléctrica Obligatorio para Todos los Microcomputadores	7.02.02.01	“Equipo de Protección Eléctrica”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
586	Equipo de Protección Contra Electricidad Estática y Condiciones Locales	7.02.01.05	“Protección Contra Electricidad Estática”
587	Dispersión de Sistemas Computacionales y Comunicacionales	7.02.01.06	“Dispersión de Sistemas Computacionales”
588	Servidores Web y Comerciales No Deben Almacenar Información Crítica	8.07.03.05	“Almacenamiento en Servidores Web y Comerciales”
589	Evitar Punto Central de Falla de Red de Comunicaciones	8.05.01.08	“Punto Central de Falla de la Red”
590	Diversas Rutas de Redes de Larga Distancia Obligatorias	8.05.01.09	“Múltiples Operadoras Telefónicas”
591	Cumplimiento de Normas Obligatorio para Soporte de Emergencias/Desastres	11.01.01.01	“Requerimientos para el Soporte de Emergencias y Desastres”
592	Marco de Segmentación de los Recursos Informáticos por Prioridad de Recuperación	11.01.03.01	“Clasificación de Recursos Informáticos”
593	Clasificación Anual de la Criticidad de las Aplicaciones Multiusuario	11.01.02.01	“Clasificación de la Criticidad de las Aplicaciones Multiusuario”
594	Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones	11.01.02.02	“Esquema de Clasificación en Cinco Categorías de la Criticidad de las Aplicaciones”
595	Preparación y Mantenimiento de los Planes de Respuesta ante Emergencias de Computación	8.01.03.02	“Planes de Respuesta Ante Emergencias Computacionales”
596	Presencia Continua del Personal del Centro de Computación para la Resolución Inmediata de Problemas	7.01.04.01	“Presencia del Personal del Centro de Computación”
597	Organización/Mantenimiento del Equipo de Respuesta ante Emergencias de Computación	8.01.03.03	“Equipo de Respuesta Ante Emergencias Computacionales”
598	Simulacros Regulares para Probar Equipo de Respuesta ante Emergencias de Computación	8.01.03.04	“Simulacros del Equipo de Respuesta Ante Emergencias Computacionales”
599	Acciones Obligatorias Despues de Sospecha de Intrusión en los Sistemas	8.01.03.05	“Sospecha de Intrusión en los Sistemas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
600	Personal de Operaciones Debe Tener Procedimiento Documentado de Respuesta a Intrusión	8.01.03.06	“Procedimientos de Respuesta a Intrusión”
601	Monitoreo Regular de Alertas sobre Vulnerabilidades en la Seguridad Informática	8.01.03.07	“Alertas Sobre Vulnerabilidades”
602	Sistema de Alerta de Seguridad Informática	8.01.03.08	“Sistema de Alerta de Seguridad Informática”
603	Usuarios No Deben Distribuir Información Acerca de las Vulnerabilidades del Sistema	6.03.02.01	“Informe de Vulnerabilidades del Sistema”
604	Usuarios Deben Notificar al Centro de Atención al Usuario Acerca de Todos los Problemas del Sistema de Producción	6.03.01.05	“Problemas en el Sistema de Producción”
605	Notificación a Gerencia de Condiciones Que Pueden Interrumpir el Trabajo	6.03.02.02	“Condiciones de Interrupción”
606	Se Espera la Asistencia del Empleado Mientras se Restauran las Actividades del Negocio	11.01.04.02	“Expectativas sobre el Empleado Durante la Restauración de las Actividades del Negocio”
607	Inventario de Puestos Técnicos Esenciales y los Individuos Que los Pueden Ocupar	8.01.01.06	“Puestos Técnicos Esenciales”
608	Adiestramiento Multidisciplinario en Puestos Técnicos Esenciales	8.01.01.07	“Adiestramiento Multidisciplinario”
609	Preparación y Mantenimiento de Planes de Recuperación Ante Desastre Computacional	8.01.01.05	“Planes de Recuperación Ante Desastre Computacional”
610	Preparación y Mantenimiento de Planes de Contingencia Empresarial	11.01.03.02	“Preparación y Mantenimiento de Planes de Contingencia Empresarial”
611	Proceso de Planificación de Continuidad de Negocios y Computación	11.01.04.01	“Plan de Continuidad de Negocios y Computación”
612	Reversión a Procedimientos Manuales Cuando Sea Posible por Costos	11.01.05.01	“Reversión a Procedimientos Manuales”
613	Inventario Anual de Hardware, Software, Etc., en Sistemas Informáticos	5.01.01.02	“Inventario de Activos — Tecnología”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
614	Números de Serial de Equipos Con los Que Los Custodios Deben Controlar Inventario	5.01.01.03	“Control de Inventario”
615	Nivel de Determinación Anual de los Niveles de Soporte de Emergencias/Desastres	11.01.05.03	“Niveles de Soporte de Interrupción del Negocio”
616	Prueba de Planes de Contingencia del Sistema Computacional y Comunicacional	11.01.05.04	“Prueba del Plan de Contingencia”
617	Mantenimiento Preventivo de los Sistemas Computacionales y Comunicacionales	7.02.04.02	“Mantenimiento Preventivo”
618	Requerimientos de Mantenimiento de los Equipos de los Sistemas Informáticos	7.02.04.03	“Mantenimiento de Equipos”
619	Deben Confirmarse los Pagos de Registro de los Nombres de Dominios en Internet	8.05.01.10	“Registros de Nombres de Dominio en Internet”
620	Números de Contacto para Empleados del Departamento de Sistemas Informáticos	8.01.01.08	“Información de Contacto”
621	Sistemas de Control de Acceso a la Información para los Procesos de Restauración de Archivos de Usuarios Finales	9.05.05.10	“Control de Acceso para Restaurar Archivos”
622	Qué Datos Respalдар y Frecuencia Mínima de Respaldo	8.04.01.02	“Respaldo de Datos”
623	Respaldos Periódicos y Suplementarios Requeridos para Computadores Portátiles	8.07.05.22	“Respaldo de Computadores Portátiles”
624	No Usar Discos Duros para Respaldo en Computadores de Acceso Público	8.04.01.03	“Medios de Respaldo”
625	Cifrado en Medios de Respaldo Almacenados Fuera de Sede	8.04.01.04	“Cifrado en Medios de Respaldo”
626	Dos Copias de la Información Sensible, Crítica o Valiosa	8.07.05.23	“Copias de Información Sensible, Crítica o Valiosa”
627	Dos Copias de Registros Críticos de la Empresa X Almacenados Fuera de Sede	8.04.01.06	“Copias Múltiples de Respaldo”
628	Revisión Gerencial del Proceso de Respaldo del Usuario Final	8.07.05.24	“Revisión del Respaldo”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
629	Especificación del Proceso de Respaldo y Frecuencia	8.04.01.07	“Proceso de Respaldo”
630	Respaldo Automático al Servidor de Red de Area Local	8.04.01.08	“Respaldos Automáticos”
631	Usuarios Notificados de que Todos los Datos se Respaldan Rutinariamente	8.04.01.09	“Revisión de la Información Respaldada”
632	Hacer Por los Menos Una Copia de los Archivos Críticos Respaldados Antes de Usar	8.04.01.10	“Archivos Críticos de Respaldo”
633	Procesamiento en Lote Sólo Si Se Completa Respaldo de Pre-Procesamiento	8.04.01.11	“Respaldo Antes del Procesamiento”
634	Auditorías Anuales para Determinar Si Se Realiza Respaldo de Producción	12.02.02.01	“Auditorías de Respaldo de Producción”
635	Almacenamiento Fuera de Sede de Medios de Respaldo	8.04.01.12	“Almacenamiento de Medios de Respaldo”
636	Medios de Respaldo Almacenados en Distintas Zonas de Riesgo Desde Máquina Originaria	8.04.01.13	“Distintas Zonas de Riesgo de Incendio”
637	Sitios de Almacenamiento de Medios de Respaldo Deben Estar Bajo Llave	8.04.01.14	“Almacenamiento de Medios de Respaldo”
638	Almacenamiento de Archivos de Cada Versión de los Sitios Web y Comerciales en Internet	8.04.01.15	“Archivos de Sitios Web y Comerciales”
639	Respaldos de Archivos Trimestrales Obligatorios para Toda Información Crítica	8.04.01.16	“Respaldo de Información Crítica”
640	Gerentes Departamentales Deben Identificar Registros Vitales	12.01.03.05	“Identificación de Registros Vitales”
641	Directorio de la Información Mantenida en Almacenamiento de Archivos	8.04.01.17	“Directorio de Almacenamiento de Archivos”
642	Medios Aceptables de Almacenamiento de Archivos	8.04.01.18	“Medios de Almacenamiento de Archivos”
643	Pruebas Regulares de los Medios de Almacenamiento de Archivos	8.04.01.19	“Pruebas de Medios de Almacenamiento de Archivos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
644	Pruebas Regulares de Medios Usados de Datos Empleados para el Almacenamiento de Archivos	8.04.01.20	“Calidad de los Medios de Almacenamiento de Archivos”
645	Preservación de los Datos Contenidos en el Almacenamiento de Archivos	8.04.01.21	“Preservación del Almacenamiento de Archivos”
646	Período Mínimo de Retención de la Información	12.01.03.07	“Período de Retención de la Información”
647	Definición del Cronograma de Retención de los Archivos en Almacenamiento	12.01.03.08	“Cronograma de Retención de los Archivos Almacenados”
648	Responsabilidad por el Cronograma de Retención de los Archivos Almacenados	12.01.03.09	“Cronograma de Retención de Datos”
649	Requerimientos para la Retención de los Datos del Documento Fuente	12.01.03.10	“Retención del Documento Fuente”
650	Período de Retención de los Datos del Documento Fuente	12.01.03.11	“Período de Retención del Documento Fuente”
651	Depuración Regular de Información Ya No Necesaria	12.01.03.13	“Destrucción de Información”
652	Procedimiento para Liberar Equipos y Medios Usados a Terceros	7.02.06.01	“Liberación de Componentes Usados”
653	Destrucción de Información y Disposición de Equipos de Sistemas Informáticos	7.02.06.02	“Disposición de Información y Equipos”
654	Destrucción de Registros o Información Requiere de Autorización Gerencial	12.01.03.14	“Destrucción de Registros”
655	Destrucción de Registros Prohibida A Menos Que Esté Autorizada por Lista o Cronograma	12.01.03.15	“Cronograma de Destrucción de Registros”
656	Proceso de Destrucción de Datos En Espera por Descubrimiento	12.01.03.16	“Moratoria en Destrucción de Datos”
657	Gerencia Debe Ser Notificada de los Atributos de la Integridad de la Información	12.03.01.01	“Atributos de la Integridad de la Información”
658	Notificación a la Gerencia de Falla en los Controles de la Integridad de la Información	6.03.03.01	“Notificación de Falla en los Controles de la Integridad”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
659	Receptores de Cálculos Deben Recibir Información Para Verificar Exactitud	8.07.03.06	“Verificación del Cálculo de la Cuenta”
660	Naturaleza de las Modificaciones a la Información Debe Ser Divulgada	8.06.03.10	“Divulgación de las Modificaciones a la Información”
661	Etiquetas de Fuente y Fecha Obligatorias para Decisiones Importantes	5.02.02.36	“Etiquetado de Datos Usados Como Base de Decisión Gerencial”
662	Supresión o Etiquetado de Información Incompleta U Obsoleta	5.02.02.37	“Información Incompleta u Obsoleta”
663	Transacciones de Producción Deben Tener Números Secuenciales	10.02.03.01	“Autorización para Transacciones en Sistema de Producción”
664	Autorización Requerida para Todas las Transacciones de Entrada al Sistema de Producción	10.02.03.02	“Validación de Entrada Rechazada o Suspendida”
665	Cambios en la Sensibilidad, Criticidad y Valor de la Información	10.02.02.06	“Cambios en la Sensibilidad, Criticidad y Valor de la Información”
666	Valdación de Datos de Entrada y Manejo de Item Rechazado	10.02.01.02	“Validación de Datos de Entrada y Manejo de Item Rechazado”
667	Cambio de Correo Electrónico y Dirección Regular Confirmado Via Dirección Anterior	8.07.05.25	“Confirmación de Cambio de Dirección”
668	Se Exige Doble Tecla Para Todos los Montos Que Excedan \$1,000	10.02.01.03	“Entrada con Doble Tecla de Transacciones Mayores”
669	Numeración de Líneas Obligatoria para Mensajes de Texto Críticos	8.07.05.26	“Numeración de Líneas en Mensajes Críticos”
670	Originador de Transacciones Debe Estar Claramente Identificado	10.02.01.04	“Originador de Transacciones”
671	Entrada en Almacén de Datos Requiere Etiquetas de Fuente, Clasificación y Otras	5.02.01.23	“Etiquetas de Entradas en Almacén de Datos”
672	Documentos Oficiales Preparados a Mano Deben Utilizar Tinta Exclusivamente	5.02.02.38	“Documentos Oficiales Preparados a Mano”
673	Revisión de Análisis Computarizados Realizados por Individuos	8.01.04.04	“Revisión de Análisis Computarizados”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
674	Controles Para Datos Utilizados para Alcanzar Decisiones Que Involucran \$100,000.	10.02.02.07	“Validación de los Controles”
675	Riesgo Aceptable de Alteración No Detectada de la Información	4.01.01.01	“Alteración No Detectada de la Información”
676	Fotografías Alteradas Deben Estar Etiquetadas Como Tales	5.02.02.39	“Fotografías Alteradas”
677	Manejo de Transacciones de Entrada Rechazadas Vía Archivos en Suspensión	10.02.02.08	“Transacciones de Entrada Rechazadas”
678	Tiempo para Resolución de Componentes en Archivos en Suspensión	10.02.02.09	“Cronograma de Resolución de Archivos en Suspensión”
679	Procedimientos de Validación para Entradas Rechazadas o Suspendidas	10.02.02.08	“Transacciones de Entrada Rechazadas”
680	Información Personal Cambiada Sólo Despues de Proporcionar Valores Previos Correctos	12.01.04.95	“Modificaciones a la Información Personal”
681	Autorización para Cambios en Datos y Programas de Producción	8.01.01.09	“Cambios en Producción”
682	Todas las Transacciones de Producción Deben Estar Autorizadas por la Gerencia	8.01.01.10	“Autorización para Transacciones de Producción”
683	Revisar Racionalidad y Exactitud de Cambios a Registros Internos	10.02.04.02	“Revisión de Cambios a Registros Internos”
684	Acciones Obligatorias Despues de Detectar Errores en Registros	8.07.03.08	“Investigación de Errores”
685	Procedimientos Normalizados de Control para Corregir Registros de Negocios	8.01.01.11	“Corrección de Registros de Negocios”
686	No Deben Utilizarse Teléfonos Celulares en los Centros de Datos	7.01.04.02	“Uso de Teléfonos Celulares”
687	Representaciones de los Empleados de la Empresa X	8.07.07.20	“Representaciones de la Organización”
688	Identidad Falsa en Sistemas Electrónicos de Comunicación	8.07.06.08	“Identidades Falsas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
689	Manera Consistente de Representar la Información de Contacto del Empleado	8.06.03.11	“Información de Contacto del Empleado”
690	Necesidad de Validación Cruzada de Información Importante	8.07.06.09	“Validación Cruzada de la Información”
691	Todas las Representaciones Públicas Deben Ser Aprobadas por Relaciones Públicas	8.07.07.21	“Aprobación de las Representaciones Públicas”
692	Derecho a Libre Expresión No Se Aplica a los Sistemas de la Empresa X	8.07.05.27	“Derecho a la Libre Expresión”
693	Derecho a Censurar Datos en Sistemas de la Organización	8.07.05.28	“Censura de Datos”
694	Nuevos Tipos de Información Deben Ser Reflejados en el Diccionario Corporativo de Datos	5.01.01.04	“Diccionario de Datos”
695	Derecho a Quitar Material Ofensivo sin Aviso	8.07.05.29	“Remoción de Material Ofensivo”
696	Sin Responsabilidad de Monitorear Contenido de Sistemas Informáticos	8.07.05.30	“Responsabilidad de Monitorear Contenido”
697	Prohibidos Usos de Facilidades Computacionales y Comunicacionales de la Empresa X	12.01.05.17	“Discusiones Utilizando Servicios Computacionales y Comunicacionales”
698	Excepción de Responsabilidad por Contenido de Mensajes	8.07.06.10	“Sin Responsabilidad en Mensajes”
699	Comentarios en Sistemas No Necesariamente Reflejan la Posición de la Empresa X	8.07.06.12	“Comentarios Públicos en Sistemas Electrónicos”
700	Advertencias Obligatorias Si los Receptores Pueden Ofenderse o Molestar	8.07.07.22	“Comunicaciones Potencialmente Ofensivas”
701	Toda Información en Internet Debe Poseer Etiquetas Normalizadas de Contenido	8.07.06.13	“Etiquetas de Contenido en Internet”
702	No se Proporcionan Servicios de Protección de Mensajes en Red	8.05.01.12	“Servicios de Protección de Mensajes en Red”
703	Prohibición de Ataques Sexuales, Etnicos y Raciales	6.01.04.10	“Acoso Sexual, Etnico y Racial”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
704	Conducta Restringida para Comunicaciones Salientes en Internet	8.07.06.15	“Comunicaciones Salientes en Internet”
705	Direcciones Internas de la red No Deben Ser Publicadas	8.05.01.13	“Direcciones Internas de la Red”
706	Paquetes de Control de Acceso Obligatorios para los Computadores de la Red	9.04.01.02	“Control de Acceso a Computadores de Red”
707	Paquetes de Control de Acceso para Computadores Conectados en Red	9.04.02.01	“Control de Acceso a los Computadores Conectados a la Red”
708	Redes Grandes Deben Dividirse en Dominios Separados	8.05.01.14	“Dominios en la Red”
709	Máquinas Conectadas a Internet Deben Tener Sistemas de Detección de Intrusos	8.05.01.16	“Sistemas de Detección de Intrusos”
710	Acceso Permisible a Internet Sin Cortafuegos	9.04.07.02	“Acceso a Internet Sin Cortafuegos”
711	Todos los Servidores Web de Internet Deben estar Protegidos por Cortafuegos	9.04.09.01	“Cortafuegos de Servidores Web”
712	Servidores Comerciales de Internet Deben Estar en Zonas Desmilitarizadas	8.05.01.19	“Cortafuegos de Servidores Comerciales de Internet”
713	Servidores Públicos en Internet Deben Estar en Subredes Separadas	8.05.01.20	“Servidores Públicos en Internet”
714	Servidores Comerciales en Internet Deben Utilizar Certificados Digitales y Criptografía	8.07.03.09	“Seguridad de los Servidores Comerciales en Internet”
715	Conexiones Discadas Deben Utilizar Cortafuegos	8.05.01.21	“Conexiones Discadas”
716	Conexiones de Redes Externas en Tiempo Real Requieren Cortafuegos	8.05.01.22	“Conexiones a Redes Externas en Tiempo Real”
717	Cortafuegos Deben Estar Configurados de Tal Manera Que Todos los Servicios Se Nieguen A Menos Que Estén Autorizados	8.05.01.23	“Configuración de Cortafuegos”
718	Cortafuegos Deben Ejecutarse en Computadores Dedicados	8.05.01.24	“Computadores para Cortafuegos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
719	Cambio de la Configuración del Cortafuego Requiere Autorización de Seguridad Informática	8.05.01.25	“Cambios a Configuración de Cortafuegos”
720	Connexiones a Internet Requieren de Cortafuegos Aprobados	8.05.01.26	“Conexiones a Internet”
721	Se Prohiben Relaciones de Confianza en Máquinas Conectadas a Internet	8.05.01.27	“Sistemas de Directorios Compartidos”
722	Conexiones Directas a la Red con Organizaciones Externas (Túneles)	8.05.01.28	“Conexiones en Red con Organizaciones Externas”
723	Prohibidos los Comandos Inter-Procesador Desde Ubicaciones Externas	9.04.03.06	“Comandos Inter-Procesador”
724	Aislar Sistemas de la Red Con Información Secreta	9.06.02.02	“Aislamiento de Sistemas con Información Secreta”
725	Clientes Deben Específicamente Estar de Acuerdo con Recibir Servicio Nuevo/Mejorado	8.07.03.10	“Servicio Nuevo o Mejorado”
726	Autorización Previa Requerida para Todos los Cambios en la Línea de Comunicación	8.05.01.29	“Cambios en la Línea de Comunicación”
727	Autorización Previa Requerida para Instalar Sistemas Multiusuario	8.02.01.01	“Implantación de Sistemas Multiusuario”
728	Autorización Previa Requerida Para Interconexión de Sistemas Internos	8.02.01.02	“Interconexión de Sistemas”
729	Subred Separada Requerida para Conexiones Personales a la Red	9.04.06.01	“Conexiones Personales a la Red”
730	Prohibidos Puertos de Red Activos Desatendidos en Areas Públicas	9.04.07.03	“Acceso Público a Puertos Activos de la Red”
731	Puertos de Red en Oficinas Vacías Deben Ser Desactivados	9.04.07.04	“Puertos de Red en Oficinas Vacías”
732	Configuración para Evitar/Detectar Conexiones No Autorizadas a la Red	8.05.01.30	“Configuración de Conexiones a la Red”
733	Criterios para Conectar Redes de la Empresa X a Redes de Terceros	9.04.02.02	“Conexiones a Redes de Terceros”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
734	Requerimientos de Seguridad para Sistemas de Terceros Conectados a la Red	4.02.02.11	“Sistemas de Terceros Conectados a la Red”
735	Autorización Requerida para Establecer Conexión con Internet	9.04.01.03	“Autorización para Conexiones a Internet”
736	Criterios de Seguridad Como Prerrequisitos Para Conexión a Intranet	8.05.01.31	“Criterios de Seguridad para Conexión a Intranet”
737	Inventario de Conexiones a Redes Externas	8.05.01.32	“Inventario de Conexiones a Redes Externas”
738	No Se Aplican Normas de Telefónicas Comunes	9.04.01.04	“Normas de Telefónicas Comunes”
739	Participación en Redes Públicas como Proveedor de Servicios	8.05.01.33	“Provisión de Servicios de Redes Públicas”
740	Formación de Contratos Obligatorios Vía Sistemas Electrónicos	8.07.03.11	“Contratos Obligatorios en Sistemas Electrónicos”
741	Negocios por Internet con Compañías Extranjeras	8.07.03.12	“Transacciones Internacionales de Negocios por Internet”
742	Convenio con Socios Antes de Usar Redes Computarizadas	8.07.03.13	“Convenio de Redes con Socios de Negocios”
743	Sólo Empleados Designados Pueden Formar Contratos Vía Correo Electrónico	8.07.03.14	“Contratos por Correo Electrónico”
744	Criterios para Aceptar y Actuar con Transacciones Computarizadas	8.07.03.15	“Aceptación de Transacciones Computarizadas”
745	Múltiples Canales de Comunicación para las Ofertas y Aceptaciones Electrónicas	8.07.03.16	“Ofertas y Aceptaciones Electrónicas”
746	Clientes de Internet Deben Específicamente Estar de Acuerdo con Términos y Condiciones	8.07.06.16	“Términos y Condiciones en Internet”
747	Proceso de Cifrado Prohibido Salvo Que Esté Autorizado	10.03.02.01	“Autorización del Proceso de Cifrado — Sistemas”
748	Uso de Cualquier Proceso de Cifrado Requiere Autorización Escrita Previa	10.03.02.02	“Autorización de Proceso de Cifrado — Usuarios”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
749	Prohibido Usar Utilidades de Cifrado con Contraseñas o Claves del Usuario	10.03.02.03	“Contraseñas y Claves en Utilidades de Cifrado”
750	Cumplimiento de Comercio Internacional en Reglamentos de Armamentos	12.01.06.01	“Armamentos en Comercio Internacional”
751	Datos Secretos Enviados por Redes Deben Estar Cifrados	8.06.03.12	“Transmisión de Datos Secretos”
752	Transporte de Datos Secretos en Medios de Almacenamiento Legibles por el Computador	8.06.03.13	“Transporte de Datos Secretos”
753	Información Secreta Debe Estar Cifrada Cuando No se Use	8.06.03.14	“Cifrado de la Información Secreta”
754	Datos Almacenados en Disco Duro Deben Estar Cifrados	8.06.03.15	“Cifrado de Almacenamiento en Disco”
755	Algoritmo de Cifrado Normal Gubernamental e Implantación	10.03.02.04	“Algoritmo de Cifrado Normal e Implantación”
756	Algoritmos de Cifrado Utilizados Deben Ser Evaluados Públicamente (Abiertos)	10.03.02.05	“Algoritmos de Cifrado Evaluados Públicamente”
757	Divulgación de Claves de Cifrado Requiere Autorización Especial	10.03.05.01	“Divulgación de Claves de Cifrado — Autorización”
758	Sistemas de Gestión de Claves de Cifrado y Separación de Tareas	10.03.05.02	“Sistemas de Gestión de Claves de Cifrado”
759	Inicialización de Sistemas de Cifrado Requiere de Presencia de Auditor	10.03.02.06	“Inicialización del Sistema de Cifrado”
760	Condiciones para la Delegación de la Responsabilidad de la Gestión de Claves	10.03.05.03	“Delegación de la Responsabilidad en la Gestión”
761	Protección de Claves Raíces de Certificados Digitales ante Autoridades de Certificación	10.03.05.05	“Protección de Claves Raíces de Certificados Digitales”
762	Canales Distintos de Comunicación para Datos y Claves de Cifrado	10.03.05.06	“Transmisión de Datos y Claves de Cifrado”
763	Sistemas Automáticos de Gestión de Claves de Cifrado Preferidos	10.03.05.07	“Gestión Automática de Claves de Cifrado”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
764	Vida Máxima de Claves de Cifrado	10.03.05.08	“Ciclo de Vida de Claves de Cifrado”
765	Definición de Ciclo de Vida para Todas las Claves de Cifrado	10.03.05.09	“Vencimiento de Claves de Cifrado”
766	Proceso para Generar Claves de Cifrado	10.03.05.10	“Generación de Claves de Cifrado”
767	Longitud Mínima de Claves de Cifrado Seleccionadas por Usuarios	10.03.05.11	“Longitud de Claves de Cifrado Seleccionadas por Usuarios”
768	Protección para los Materiales de Generación de Claves de Cifrado	10.03.05.12	“Materiales para la Generación de Claves”
769	Protección para Claves Maestras de Cifrado en Texto	10.03.05.13	“Claves Maestras de Cifrado en Texto”
770	Destrucción de los Materiales de Generación de Claves de Cifrado	10.03.05.14	“Destrucción de Materiales para Generación de Claves”
771	Cronograma para la Destrucción de los Materiales de Intercambio de Claves	10.03.05.15	“Destrucción de Material de Intercambio de Claves”
772	Período de Protección de las Claves de Cifrado Usadas para Confidencialidad	10.03.05.16	“Segreto de la Clave de Cifrado”
773	Período de Protección de las Claves de Firmas Digitales Privadas	10.03.05.17	“Ciclo de Vida de las Claves Privadas de Firmas Digitales”
774	Nunca Respaldar Automáticamente Clave Privada Usada para Certificados Digitales	10.03.05.18	“Respaldos de Claves Privadas”
775	Duplicación de Claves de Cifrado para Datos Que Han Sido Respaldados	10.03.05.19	“Duplicación de Claves de Cifrado”
776	Prevención de Divulgación No Autorizada de Claves de Cifrado	10.03.05.20	“Divulgación de Claves de Cifrado — Controles”
777	Clave Privada para Certificados Digitales Debe Estar Cifrada o en Tarjeta Inteligente	10.03.05.21	“Seguridad de Clave Privada para Certificados Digitales”
778	Prohibida Transmisión de Claves de Cifrado Privadas en Texto	10.03.05.23	“Transmisión de Claves de Cifrado Privadas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
779	Notificar a Corresponsales Acerca de Cambios en Claves Públicas	10.03.05.24	“Cambios en Claves Públicas”
780	Claves Comprometidas Revocadas a Ultima Instancia Donde Eran Seguras	10.03.05.25	“Claves Comprometidas”
781	Prohibido Almacenamiento de Claves de Cifrado en los Mismos Medios que los Datos Protegidos	10.03.05.26	“Medios de Almacenamiento de Claves de Cifrado”
782	Claves de Cifrado de Respaldo Proporcionadas al Oficial de Seguridad Informática	10.03.05.28	“Claves de Cifrado de Respaldo”
783	Sistemas Generales de Cifrado Deben Incluir Clave en Garantía	10.03.04.01	“Sistemas de Cifrado de Propósito General”
784	Claves de Firmas Digitales y de Autenticación de Usuarios No Deben Ponerse en Garantía	10.03.05.30	“Claves de Firmas Digitales y de Autenticación de Usuarios”
785	Claves Distintas para Cifrado y Firmas Digitales	10.03.05.31	“Separación de Claves de Cifrado y de Firmas Digitales”
786	Asignación Explícita de las Funciones de Gestión de las Claves de Cifrado	10.03.05.32	“Responsabilidad de la Gestión de Claves”
787	Eliminación de Datos Legibles Después de Hacerse una Versión Cifrada	10.03.02.07	“Eliminación de Datos Fuente Después de Cifrar”
788	Compresión y Cifrado de Datos Confidenciales a Almacenar	10.03.02.08	“Compresión y Cifrado de Datos Secretos”
789	Módulos de Hardware Resistentes para Procesos de Cifrado	10.03.02.09	“Módulos de Hardware para el Proceso de Cifrado”
790	Inserción de Números de Acceso a los Computadores en Directorios	8.05.01.34	“Números de Acceso a Computadores”
791	Cambios Periódicos de Números de Comunicación de Computadores	8.05.01.35	“Cambio de Números Discados”
792	Sistemas Extendidos de Autenticación Requeridos para Líneas Discadas	9.04.03.07	“Autenticación de Usuario Que Accede Vía Telefónica”
793	Identidad de Usuario al Exterior Debe Autenticarse Antes de Establecer Sesión	8.05.01.36	“Conexiones Salientes”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
794	Uso de Modems de Cable para Comunicaciones de Negocios	8.05.01.37	“Modem por Cable”
795	Modem en Estaciones de Trabajo Conectadas a Redes Internas	9.04.02.03	“Modem de Estaciones de Trabajo”
796	Conexiones de Discado Directo Prohibidas A Menos Que Se Use Pool de Modem	9.04.02.04	“Conexiones de Discado Directo”
797	Registro de Todas las Líneas de Modem y Proceso Correspondiente de Autorización Previo	9.04.02.05	“Registro de Línea de Modem”
798	Autorización Requerida para Sistemas Que Aceptan Llamadas Discadas Entrantes	9.04.04.01	“Sistemas Que Aceptan Llamadas Discadas Entrantes”
799	Prohibición de Modem de Computadores Personales en Modo Auto-respuesta	9.04.02.06	“Modem en Auto-Respuesta”
800	Llamadas Discadas Entrantes No Deben Responderse Hasta Cuarta Campanada	8.05.01.38	“Configuración de Modem para Llamadas Discadas Entrantes”
801	Gerencia Departamental Responsable de Cumplimiento en Discado	12.02.01.01	“Cumplimiento del Discado Telefónico”
802	Máximo de Intentos de Contraseñas Permisibles para Usuarios de Discado	9.04.03.08	“Intentos de Contraseñas por Discado”
803	Proceso para Descargar Software Desde Un Sitio Espejo en Internet	8.03.01.22	“Descarga de Software Desde Un Sitio Espejo en Internet”
804	Controles Necesarios para Descargar Información Sensible de la Empresa X	8.06.03.16	“Descarga de Información Sensible”
805	Prohibido Descargar Información Sensible Sin Permiso	8.06.03.17	“Autorización para Descargar Información Sensible”
806	Sincronización Automática de Dispositivos Permitida Sólo con Permiso	8.07.05.31	“Sincronización de Dispositivos”
807	Prohibidas Llamadas Con Cobro a Destino y de Terceros en Líneas de Correo Voz	8.07.05.32	“Llamadas Cobro a Destino y a Terceros”
808	Inhabilitar Código de Area 900 en Todos los PBX de la Empresa X	8.07.05.33	“Llamadas a Servicios de Información”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
809	Areas Definidas en PBX Deben Ser Restringidas	8.07.05.34	“Areas Telefónicas”
810	Trabajadores No Deben Regresar Llamadas de Larga Distancia	8.06.03.18	“Devolución de Llamadas de Larga Distancia”
811	Solicitudes Inusuales de Operación Telefónica Deben Ser Denegadas y Reportadas	8.06.03.19	“Solicitudes Inusuales de Operación Telefónica”
812	Dejar Información Sensible en Contestadoras	8.07.07.23	“Información Sensible en Máquinas Contestadoras”
813	Contraseñas de Correo Voz No Sujetas a Normas de Construcción	9.03.01.20	“Construcción de Contraseñas de Correo Voz”
814	Mensajes de Voz Escuchados Eliminados Despues de Almacenados Durante Un Mes	8.07.05.35	“Almacenamiento de Mensajes de Correo Voz”
815	Llamadas por Tarjeta de Crédito a Través de Sistemas PBX	8.07.05.36	“Llamadas con Tarjeta de Crédito”
816	Uso de Tarjetas de Crédito en Teléfonos Públicos	8.07.07.24	“Uso de Tarjetas de Crédito”
817	Características DISA del PBX Requieren Facilidades de Detección de Fraudes	8.07.05.37	“Implantación del Acceso al Sistema Telefónico Directo”
818	Guía Telefónica Contiene Información Restringida	4.02.01.10	“Guías Telefónicas Internas”
819	Obligatorio Consentimiento de Ambas Partes para Usar Altavoces Telefónicos y Grabadores	8.07.07.25	“Uso de Tecnología Telefónica para Conferencias o Grabación”
820	Permiso Especial Necesario para Grabar Sesiones de Videoconferencias	8.07.07.26	“Grabación de Videoconferencias”
821	Uso de Teléfonos para Asuntos Personales	8.06.03.20	“Uso Personal del Teléfono”
822	Reembolso por Llamadas Telefónicas Personales	8.06.03.21	“Llamadas Telefónicas Personales de Larga Distancia”
823	Registros Exactos para Evitar Telemercadeo No Deseado	8.07.03.17	“Registros de Telemercadeo”
824	Ordenes para Cambiar Registros Internos por Vía Telefónica	8.07.05.38	“Ordenes para Cambiar Registros”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
825	Puente de Conferencia Activado Sólo Durante Su Uso	8.07.05.39	“Activación del Puente de Conferencias”
826	Códigos de Identificación para el Soporte Técnico	9.05.03.06	“Códigos de Identificación para Soporte Técnico”
827	Uso de una Cuenta de Correo Electrónico Asignada a Otra Persona	9.03.01.21	“Cuentas Unicas de Correo Electrónico”
828	Uso de Direcciones Electrónicas de Correo Distintas a la Oficial	8.07.04.03	“Direcciones de Correo Electrónico”
829	Información de Contacto del Remitente Debe Incluirse en Correo Electrónico	8.07.04.04	“Información de Contacto del Remitente”
830	Fuente Claramente Identificada de Material de Mercadeo por Correo Electrónico	8.07.04.05	“Fuente de Material de Mercadeo por Correo Electrónico”
831	Reenvío Electrónico A Dirección de Red Externa	8.07.04.06	“Reenvío Externo de Correo Electrónico”
832	Reenvío de Mensajes Electrónicos Externos	8.07.04.07	“Mensajes de Correo Electrónico Inadecuados”
833	Grabación y Retención de Correo Electrónico	8.07.04.08	“Manejo de Mensajes de Correo Electrónico”
834	Retención de Mensajes de Correo Electrónico para Referencia Futura	8.07.04.09	“Retención de Mensajes de Correo Electrónico”
835	Usuarios No Deben Emplear Sistemas de Correo Electrónico Como Base de Datos	8.07.04.10	“Almacenamiento de Mensajes de Correo Electrónico”
836	Destrucción Periódica de Mensajes de Correo Electrónico Archivados	8.07.04.11	“Destrucción de Mensajes de Correo Electrónico”
837	Expectativas de Privacidad y el Correo Electrónico	8.07.04.12	“Privacidad en Correo Electrónico”
838	Ver Correo Electrónico Como Comunicaciones Públicas	8.07.04.14	“Cifrado de Correo Electrónico”
839	Autorización para Leer Mensajes de Correo Electrónico de Otros Trabajadores	8.07.04.15	“Autorización para Monitorear Mensajes de Correo Electrónico”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
840	Prohibido Modificar Contenido de Mensaje o Encabezado de Correo Electrónico	8.07.04.16	“Modificación de Correo Electrónico”
841	Comentarios Groseros, Obscenos o Peyerativos en Correo Electrónico	8.07.04.17	“Contenido de Mensaje de Correo Electrónico”
842	Restricciones sobre Contenido de Mensaje para Sistemas Informáticos de Empresa X	8.07.04.18	“Restricciones en Contenido de Mensajes”
843	Notificación de Monitoreo de Contenido para Transmisiones de Correo Electrónico	8.07.04.19.	“Monitoreo de Contenido de Correo Electrónico”
844	Reporte de Correo Electrónico Ofensivo a Origen y Departamento de Recursos Humanos	6.03.01.07	“Mensajes Ofensivos de Correo Electrónico”
845	Envío de Mensajes Personales de Correo Electrónico No Solicitados Despues de Solicitud de Parar	8.07.04.20	“Mensajes Personales No Solicitados de Correo Electrónico”
846	Prohibición de Correos Electrónicos Publicitarios No Deseados en Grandes Volúmenes (SPAM)	8.07.04.21	“Correo Electrónico en Volumen”
847	Reenvío como Respuesta Adecuada Ante Correo Basura (SPAM)	8.07.04.22	“Respuesta a Correo Electrónico No Solicitado”
848	Envío de Grandes Cantidad de Correo Electrónico No Solicitado (Bombardeos)	8.07.04.23	“Envíos de Correos Electrónicos No Solicitados”
849	Mensajes de Correo Electrónico Son Registros de la Empresa	8.07.04.26	“Monitoreo de Mensajes de Correo Electrónico”
850	Todo Correo Electrónico Archivado y Sujeto a Revisión de Supervisores	8.07.04.27	“Archivo y Revisión de Correo Electrónico”
851	Reenvío de Copias de Correo Electrónico Oficial a Registros de Archivo	8.07.04.29	“Archivo de Correo Electrónico”
852	Uso Personal de Sistemas de Correo Electrónico	8.07.04.30	“Usos del Sistema de Correo Electrónico”
853	Autorización Para Emitir Transmisiones en Correo Electrónico y Correo Voz	8.07.05.41	“Transmisiones a Través de Correo Electrónico y Correo de Voz”
854	Autorización Para Emitir Correo Electrónico o Correo Voz a Grupos	8.07.05.42	“Correo de Voz para Grupos”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
855	Colocación en Lista de Distribución de Correo Electrónico Requiere Consentimiento	8.07.04.31	“Distribuciones de Correo Electrónico”
856	Prohibición de Uso de Copias de Firmas Hechas a Mano	8.07.04.32	“Firmas en Correo Electrónico”
857	Prohibición de Abrir Anexos A Menos Que Se Esperen	8.07.04.33	“Anexos de Correo Electrónico”
858	Prohibidos Anexos Entrantes a Correo Electrónico por Internet	8.07.04.34	“Anexos Entrantes de Correo Electrónico”
859	Capacidades del Explorador del Correo Electrónico No Deben Utilizarse en el Negocio	8.07.06.17	“Capacidades del Explorador del Correo Electrónico”
860	Operadores de Entrada de Datos Deben Emplear Clientes Sin Carga	9.08.02.01	“Operadores de Entrada de Datos”
861	Equipo Permisible para Teletrabajo	9.08.02.02	“Equipo de Teletrabajo”
862	Alteración/Expansión de Computadores Proporcionados por Empresa X	7.02.04.05	“Modificaciones a Computadores”
863	Reporte de Daños a Sistemas Fuera de Sede de la Empresa X	6.03.01.08	“Daño y Pérdida de Sistemas Fuera de Sede”
864	Protección de Propiedad de Empresa X en Sitios Alternativos de Trabajo	9.08.01.09	“Propiedad de la Organización en Sitios Alternativos de Trabajo”
865	Derechos Sobre Propiedad Intelectual Desarrollada Fuera de Sede	6.01.04.11	“Propiedad Intelectual Desarrollada Fuera de Sede”
866	Información Almacenada en Computadores Portátiles Propiedad de la Empresa X	9.08.01.10	“Información Almacenada en Computadores Portátiles Propiedad de la Organización”
867	Teletrabajadores y Ambientes Estructurados de Trabajo	9.08.02.03	“Ambientes de Teletrabajo”
868	Uso en Sede de Sistemas de Computación Pertenecientes a Trabajadores	7.02.01.08	“Sistemas de Computación Pertenecientes a Trabajadores”
869	Requisitos de Seguridad para Trabajar en Casa	9.08.02.04	“Requisitos de Seguridad para Teletrabajo”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
870	Retención de Información Sensible para su Destrucción Vía Métodos Aprobados	12.01.03.17	“Retención de Información Sensible para su Destrucción”
871	Procedimientos de Seguridad Informática en Sistemas Remoto de Teletrabajo	9.08.02.05	“Procedimientos de Seguridad Informática en Teletrabajo”
872	Derecho a Inspeccionar Ambientes de Teletrabajo	9.08.02.06	“Inspección de Ambientes de Teletrabajo”
873	Curso de Adiestramiento Requerido Antes de Usar Sistemas de Acceso Remoto	6.02.01.03	“Adiestramiento para Acceso Remoto”
874	Trabajadores Deben Mantener Computadores Portátiles Consigo o Bajo Llave	9.08.01.11	“Posesión de los Computadores Portátiles”
875	Alternativas Móviles para Proteger Información de la Empresa X	9.08.01.12	“Alternativas para Computadores Móviles”
876	Acceso a Internet Requiere Completar Curso de Adiestramiento	6.02.01.04	“Adiestramiento en Internet”
877	Derechos de Internet Reservados para los que Tienen Necesidad por Negocio	9.04.01.06	“Derechos de Acceso a Internet”
878	Trabajadores Que No Realicen Investigación No Tienen Acceso a Web	9.04.01.07	“Restricción de Acceso a Internet”
879	Vencimiento de Identificadores de Usuario en Computadores con Acceso a Internet	9.02.01.19	“Vencimiento de Identificador de Usuario”
880	Empresa X Bloquea Ciertos Sitios Web No Relacionados con el Negocio	9.04.01.08	“Sitios Web No Relacionados con Negocio”
881	Recepción de Noticias de Internet para Tópicos de la Empresa X	8.07.06.18	“Fuentes de Noticias en Internet”
882	Autentificación Extendida de Usuario Requerida para Usuarios Entrantes a Internet	9.04.03.09	“Acceso Entrante a Internet”
883	Prohibidas Conexiones Telnet Con Contraseñas Fijas por Internet	8.05.01.38	“Contraseñas para Conexión Telnet”
884	Actualización de la Información de la Empresa X por Internet	8.07.06.19	“Modificación de Información por Internet”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
885	Inhabilitación de Java Dentro de los Exploradores Web de Internet	9.04.07.05	“Inhabilitación de Java”
886	Prohibida Ejecución de Programa Java A Menos Que Esté Validada Firma Digital	10.03.03.01	“Ejecución de Programa Java”
887	Cortafuegos Filtran Todo Contenido Activo (Java, Active X, Etc.)	8.05.01.40	“Filtrado de Contenido Activo”
888	Acceso a Internet por Computadores de Empresa X Debe Pasar por Cortafuego	8.05.01.41	“Acceso a Internet”
889	Excepción de Responsabilidad Debe Acompañar Todos Los Mensajes Personales en Internet	8.07.06.20	“Excepción de Responsabilidad en Mensajes Personales en Internet”
890	Representaciones en Internet Que Incluyan Afiliación de la Empresa X	8.07.06.21	“Representaciones en Internet Que Incluyan Afiliación”
891	Prohiba Participación en Grupos de Discusión y Chats en Internet	8.07.04.36	“Foros Electrónicos Públicos”
892	Representaciones en Internet Acerca de Productos y Servicios de la Empresa X	8.07.06.22	“Representaciones en Internet de Productos y Servicios”
893	Divulgación de Información Personal de Contacto en Foros Públicos en Internet	8.07.06.23	“Divulgación en Internet de Información de Contacto”
894	Declaraciones Políticas y Patrocinio de Productos /Servicios	8.07.06.24	“Declaraciones Políticas y Patrocinio de Productos o Servicios”
895	Participación en Grupos de Discusión por Internet y Divulgación de Secretos Empresariales	8.07.06.25	“Divulgación de Secretos Industriales por Internet”
896	Validación de la Identidad de Terceros en Internet	8.07.01.06	“Validación de la Identidad de Terceros”
897	Certificado Digital para Todos los Sitios Web y Comerciales de la Empresa X en Internet	10.03.03.02	“Sitios Web y Comerciales en Internet”
898	Trabajadores No Deben Esconder Su Identidad en Internet	9.04.01.11	“Identidad en Internet”
899	Respeto por la Propiedad Intelectual de Otros en Internet	9.04.01.12	“Propiedad Intelectual”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
900	Envío de Software y Otra Información Confidencial por Internet	8.07.06.27	“Transmisión por Internet de Información Sensible”
901	Remoción de Avisos Electrónicos Inapropiados en Foros Públicos	8.07.06.28	“Avisos Públicos Inadecuados”
902	Motores de Búsqueda para Detectar Sitios Web Engañosos con Nombres Similares	8.07.06.29	“Sitios Web Con Nombres Similares”
903	Publicación de Material de Empresa X en Internet	8.07.06.30	“Publicación en Internet de Material”
904	Establecimiento de Nuevos Acuerdos de Negocios Vía Internet	8.07.06.31	“Acuerdos de Negocios por Internet”
905	Sistemas de Producción Internos No Pueden Estar Conectados Directamente a Internet	8.05.01.42	“Conexiones Directas a Internet”
906	Directorios Públicos con Derechos de Escritura en Computadores de Empresa X Deben Limpiables Cada Noche	8.05.01.43	“Directorios Modificables por el Público”
907	Cifrado para Archivos Dejados en Servidores Anónimos FTP	10.03.02.11	“Información en Servidores FTP Anónimos”
908	Cifrado de Toda la Información de Pagos en Máquinas Accesibles desde Internet	8.07.03.18	“Cifrado de Información de Pagos”
909	Evitar Dar Información a Competencia a Través de Publicaciones en Redes	8.07.06.32	“Publicaciones en Redes”
910	Manejo de Software y Archivos Descargados de Internet	8.03.01.24	“Información Descargada”
911	Transferencia de Archivos Descargados de Internet a Otro Computador	8.07.06.33	“Transferencia de Archivos Descargados”
912	Confidabilidad de la Información Descargada de Internet	8.07.06.34	“Confidabilidad de la Información de Internet”
913	Intercambios de Información por Internet	8.06.03.22	“Intercambio de Información por Internet”
914	Carga de Software a Otras Máquinas Vía Internet	8.07.06.35	“Carga de Software”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
915	Control de Usuario Sobre Información Obtenida Vía Sitios Web de Internet	9.07.02.22	“ Información Obtenida Vía Internet ”
916	Aceptación de Ideas No Solicitadas por Internet	8.07.06.36	“ Información No Solicitada en Internet ”
917	Sistemas de Producción No Deben Depender de la Información Gratis de Internet	8.07.06.37	“ Información de Internet en Sistemas de Producción ”
918	Páginas Web No Oficiales Permitidas Sólo por Contrato	8.07.06.38	“ Páginas Web No Oficiales ”
919	Responsabilidad por Contenido en Páginas Web Personales	8.07.06.39	“ Páginas Web Personales ”
920	Comité de Manejo de Página Web en Empresa X	8.07.06.40	“ Comisión Administradora de Página Web de Internet ”
921	Requisitos de Diseño de Página Web en Internet	8.07.06.41	“ Diseño de Página Web en Internet ”
922	Se Requiere Autorización Gerencial para Establecer Enlaces Calientes en Internet	8.07.06.42	“ Establecimiento de Enlaces Calientes en Internet ”
923	Enlaces Calientes Hacia Internet Deben Estar Acompañados de Excepciones de Responsabilidad Legal	8.07.06.43	“ Excepción de Responsabilidad en Enlaces Calientes Hacia Internet ”
924	Revisión Diaria de Contenido y Enlaces Calientes en Página Web de Empresa X	8.07.06.44	“ Revisión de Página Web en Internet ”
925	Se Requiere Permiso de Propietario/Gerente Departamental para Publicación en Intranet	8.07.05.44	“ Publicaciones en Intranet ”
926	Todo Contenido de Intranet Es Propiedad de Empresa X	8.07.05.45	“ Propiedad del Contenido de Intranet ”
927	Verificación de Información Antes de Publicar en Intranet	8.07.05.46	“ Validación de Información en Intranet ”
928	Revisión y Prueba de Contenido Nuevo/Cambiado en Intranet	8.07.05.47	“ Revisión y Prueba de Contenido de Intranet ”
929	Proceso de Limpieza de Contenido Descargado de Internet y Trasladado a Intranet	8.07.05.48	“ Contenido de Internet Trasladado a Intranet ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
930	Sitios de Intranet No Debe Utilizar Contenido Activo No Autorizado	8.07.05.49	“Contenido Activo en Sitios Intranet”
931	Revisión de Páginas Web por Administrador Web Antes de Publicarlas en Intranet	8.07.05.50	“Revisión de Páginas Web en Intranet”
932	Toda Información Publicada en Páginas Intranet Deben Tener Propietario Designado	8.07.05.51	“Propietario de Información en la Intranet”
933	Toda Página Intranet Debe Incluir la Firma Digital del Propietario de la Información	8.07.05.52	“Firmas Digitales del Propietario de la Información”
934	Información Secreta No Debe Ser Colocada en Sistemas Internet o Intranet	8.07.06.51	“Información Secreta en la Web”
935	Intranet Revisada Trimestralmente para Confirmar Que Datos Confidenciales No Han Sido Publicados	8.07.05.53	“Revisión de Datos en Intranet”
936	Establecimiento de Servidor Intranet Requiere Autorización de Sistemas Informáticos	8.07.05.54	“Autorización para Servidor Intranet”
937	Conexiones en Tiempo Real a los Sistemas de Producción de Empresa X Vía Intranet	8.07.05.55	“Acceso a Sistemas de Producción por Intranet”
938	Autorización Requerida para Acceso a Sistemas Internos por Terceros	4.02.01.11	“Acceso de Terceros a Sistemas Internos”
939	Reenvío de Información en Intranet de Empresa X a Terceros	8.07.05.56	“Reenvío de Información de Intranet”
940	Transferencia Directa a Sitios Internet No Permitido desde Intranet	8.07.05.57	“Transferencia a Internet desde Intranet”
941	Desarrolladores de Sitios Intranet Deben Utilizar Guía de Estilo de Empresa X	8.07.05.58	“Guía de Estilo de Intranet”
942	Ocultar Números de Cuenta en Recibos de Clientes	10.02.02.10	“Ocultar Números de Cuenta de Clientes”
943	Debe Entregarse Recibo por Cada Compra o Compra Es Gratis	10.02.02.11	“Entrega de Recibo de Compra”
944	Información de Pago Nunca Entregada Completamente a Clientes	8.07.03.19	“Confirmación de Información de Pago”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
945	Divulgación de Números de Cuenta Bancaria	8.06.03.23	“Números de Cuenta Bancaria”
946	Destrucción de Recibos de Tarjetas de Crédito y Otra Información de Pago	5.02.02.40	“Eliminación de la Información de Pago”
947	Cifrado de Números de Tarjetas de Crédito y Otros Datos de Pago Cuando No Son Usados	8.07.03.20	“Cifrado de Datos de Pago”
948	Números de Tarjeta de Crédito Deben Usarse Solamente para Procesamiento de Pago	10.02.02.12	“Uso de Números de Tarjeta de Crédito”
949	Apertura de Cuenta Nueva Requiere Autenticación Robusta de Identidad	9.02.01.20	“Autentificación para Cuentas Nuevas”
950	Cualquier Fraude Demostrado Obliga al Cierre Inmediato de Cuenta Financiera	8.07.03.22	“Cuentas Involucradas en Fraudes”
951	Confirmación de Canales de Comunicación Alternativos para Transacciones	8.07.03.23	“Canal de Confirmación”
952	Saldo Diario y Conciliación de Registros Contables	8.07.03.24	“Saldo y Conciliación de Cuentas”
953	Acuse de Recibo Debe Confirmarse Antes de Activar Tarjeta de Pago	8.07.03.25	“Activación de Tarjeta de Pago”
954	Todos los Nuevos Trabajadores Deben Recibir Panfletos sobre Políticas de Seguridad Informática	6.02.01.05	“Panfleto sobre Políticas de Seguridad Informática”
955	Adiestramiento en Seguridad Informática Obligatorio para Todos los Trabajadores Informáticos	6.02.01.06	“Adiestramiento en Seguridad Informática”
956	Adiestramiento en Seguridad Informática Sólo Después de Pasar Otro Adiestramiento	6.02.01.07	“Adiestramiento Básico”
957	Avisos de Cambios en Políticas de Seguridad Informática Distribuidos a Todos los Trabajadores	6.02.01.08	“Cambios en Políticas de Seguridad Informática”
958	Departamento de Seguridad Informática Responsable de Adiestramiento Correspondiente	6.02.01.09.	“Responsabilidad en Adiestramiento”
959	Tiempo Obligatorio de Adiestramiento en Seguridad Informática	6.02.01.10	“Tiempo de Adiestramiento”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
960	Trabajo de Acuerdo con Políticas y Procedimientos de Seguridad Informática	6.02.01.11	“Convenio de Trabajo”
961	Obligatoria Asistencia a Clases de Seguridad Informática	6.02.01.12	“Clases Sobre Seguridad Informática”
962	Curso de Adiestramiento en Seguridad Informática Antes de Obtener Acceso al Sistema	6.02.01.13	“Adiestramiento para Acceso al Sistema”
963	Se Requiere Acatamiento de Código de Conducta Corporativo	6.01.04.12	“Código de Conducta Corporativo”
964	Reconocimiento Firmado de Haber Entendido el Código de Conducta	6.01.04.13	“Entendimiento del Código de Conducta”
965	Adiestramiento Obligatorio para el Usuario de Sistemas de Producción	6.02.01.14	“Adiestramiento en Sistemas de Producción”
966	Reporte Obligatorio de Incidentes de Seguridad Informática	6.03.01.09	“Informes de Incidentes”
967	Información de Investigación de Delitos Computarizados Es Legalmente Privilegiada	12.01.07.14	“Información Sobre Investigaciones de Delitos Computarizados”
968	Emisión de Mensajes para Detener a Atacantes	8.01.03.10	“Mensajes a Atacantes”
969	Inclusión de Información de Contacto en Seguridad Informática en Sitios Web	8.07.06.53	“Información de Contacto en Seguridad”
970	Informes Internos de Problemas y Violaciones de Seguridad Informática	6.03.01.11	“Informes de Violaciones y Problemas”
971	Reportes Centralizados de Problemas en Seguridad Informática	6.03.02.03	“Reportes Centralizados de Problemas”
972	Interferencia con Reportes de Problemas en Seguridad Informática	6.03.01.13	“Interferencia con Reportes de Violaciones y Problemas”
973	Protección de Trabajadores Que Reporten Problemas de Seguridad Informática	6.03.01.14	“Protección para Reportes de Violaciones y Problemas”
974	Reportes Externos de Violaciones de Seguridad Informática	6.03.01.16	“Reportes Externos de Violaciones”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
975	Reporte de Problemas a Inversionistas y Autoridades Gubernamentales	6.03.01.17	“Reporte de Violaciones y Problemas a las Autoridades”
976	Divulgación Pública y Gubernamental de Ataques a Sistemas de Computación	6.03.01.18	“Divulgación de Ataques a Sistemas de Computación”
977	Informe Inmediato de Sospecha de Infestación por Virus	6.03.03.03	“Informe de Sospecha de Virus”
978	Informe Obligatorio de Fucionamiento Incorrecto de Software	6.03.03.04	“Informe de Funcionamiento Incorrecto de Software”
979	Reporte de Cambios No Autorizados de Datos y Usos Cuestionables del Sistema	6.03.01.20	“Informes de Actividad No Autorizada”
980	Investigación Obligatoria Luego de Delito Computarizado	6.03.01.24	“Investigación de Delito Computarizado”
981	Cuándo Buscar Ayuda Ante Problemas de Accesos No Autorizados	8.01.03.09.	“Problemas por Accesos No Autorizados”
982	Retención de la Información Sobre Violaciones y Problemas de Seguridad Informática	12.01.03.18	“Retención de la Información Sobre Violaciones y Problemas de Seguridad”
983	Análisis Anual de Violaciones y Problemas de Seguridad Informática	6.03.04.01	“Análisis de Violaciones y Problemas”
984	Reportes de Problemas y Proceso de Manejo	8.04.03.01	“Informes de Problemas”
985	Diseñadores y Desarrolladores de Sistemas Deben Informar a Gerencia sobre Problemas	6.03.01.22	“Reporte de Problemas en Diseño”
986	Dependencia de Nuevos Productos de Seguridad de Sistemas	9.01.01.29	“Madurez del Producto de Seguridad”
987	Facilidad de Uso Obligatoria para Seguridad en Computadores y Comunicaciones	9.01.01.31	“Facilidad de Uso de los Controles de Seguridad”
988	Aceptación Obligatoria del Usuario de Medidas de Seguridad Informática	8.02.02.11	“Aceptación del Usuario de las Medidas de Seguridad Informática”
989	Incorporación de la Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas	10.01.01.09	“Seguridad en el Ciclo de Vida del Desarrollo de los Sistemas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
990	Procura de Hardware/Software Vía Canales Normales de Compras	5.01.01.05	“ Procura de Hardware y Software ”
991	Protección Consistente de la Información Sin Importar Su Naturaleza	3.01.01.01	“ Protección de la Información ”
992	Prohibido Todo Privilegio en Sistemas Informáticos No Específicamente Permitido	9.01.01.32	“ Uso de Derechos en Sistemas Informáticos ”
993	Minimización de Dependencia de Mecanismos Comunes para los Controles	10.01.01.10	“ Dependencia de Mecanismos Comunes para los Controles ”
994	Sistemas de Seguridad Independientes para Cada Sistema de Computación	9.01.01.33	“ Sistemas de Seguridad Independientes ”
995	Computadores y Redes Dedicados para Alta Seguridad/Alta Confiabilidad	9.04.06.02	“ Computadores y Redes de Alta Seguridad y Alta Confiabilidad ”
996	Controles Diseñados Con Gran Margen de Error	10.02.02.13	“ Diseño de Controles de Seguridad Informática ”
997	Uso de Versiones Más Actuales de Sistema Operativo	8.01.02.07	“ Versiones de Sistemas Operativos ”
998	Ultima Versión de Software en Sistemas en Interface con Redes Externas	8.05.01.46	“ Sistemas en Interface con Redes Externas ”
999	Medidas de Seguridad de Red No Deben Ser Compatibles Hacia Atrás	8.05.01.47	“ Medidas de Seguridad de la Red ”
1000	Mantener la Funcionalidad de la Seguridad Fuera de la Producción	10.01.01.11	“ Funcionalidad de la Seguridad en las Aplicaciones del Negocio ”
1001	Sistemas Deben Ser Configurados y Personalizados De Acuerdo con Plantillas	8.02.02.12	“ Plantillas para Configuración de Sistemas ”
1002	Evaluaciones de Riesgo Obligatorias para Sistemas Informáticos de Producción	4.01.05.01	“ Evaluación del Riesgo en los Sistemas de Producción ”
1003	Cuándo Realizar Evaluaciones de Riesgo de la Seguridad de los Sistemas Informáticos	12.02.02.02	“ Evaluaciones de Riesgo de la Seguridad de Sistemas Informáticos ”
1004	Software de Identificación de Vulnerabilidades para Sistemas Conectados a Internet	12.03.02.02	“ Identificación de Vulnerabilidades ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1005	Comprar en Lugar de Construir Soluciones de Seguridad Informática	10.01.01.12	“ Compra de Soluciones de Seguridad Informática ”
1006	Las Mejores Soluciones para Funciones Críticas de Seguridad Informática	4.01.03.05	“ Productos y Servicios de Seguridad ”
1007	Cumplimiento de Normas de Seguridad Informática Específicos a Cada Industria	3.01.01.10	“ Normas de Seguridad Informática Específicas a Cada Industria ”
1008	Marco Legal de las Políticas de Seguridad Informática	3.01.01.05	“ Conflictos Legales ”
1009	Proceso de Aceptación del Riesgo y Excepciones Permisibles a la Políticas	3.01.01.09	“ Excepciones a las Políticas ”
1010	No Obligar a Su Cumplimiento No Constituye Consentimiento	3.01.01.07	“ Sin Obligación de Hacer Cumplir las Políticas ”
1011	Controles Mínimos de Sistemas Informáticos Dictados por Prácticas Normales	10.01.01.13	“ Controles Mínimos en Sistemas Informáticos ”
1012	Respuesta Requerida para Cada Riesgo Significativo de Seguridad Informática	4.01.02.01	“ Riesgos Significativos para la Seguridad Informática ”
1013	Autorización Antes de Inhabilitar Componentes Críticos de la Infraestructura de Seguridad	4.01.04.02	“ Inabilitación de Componentes Críticos de Seguridad ”
1014	Debe Mantenerse Una Adecuada Cobertura para la Seguridad Informática	4.01.02.02	“ Cobertura de Seguros ”
1015	Asignación de Suficientes Recursos para Atender Seguridad Informática	4.01.03.06	“ Recursos para la Seguridad Informática ”
1016	Seguridad Informática Es Gasto General, No Un Cargo Reversible	4.01.03.07	“ Partida Presupuestaria para la Seguridad Informática ”
1017	Debe Poderse Obligar al Cumplimiento de las Medidas de Seguridad Antes de Implantarlas	3.01.02.01	“ Cumplimiento Forzoso de los Controles de Seguridad ”
1018	Cuando Estén Disponibles, Se Requiere el Uso de Productos Evaluados	10.01.01.14	“ Uso de Productos Evaluados ”
1019	Convenios con Terceros Que Manejan Información de la Empresa X	4.02.02.12	“ Convenios con Terceros ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1020	Acuerdos con Terceros Requieren Plan y Prueba de Respaldo	4.03.01.04	“ Planes de Contingencia para Proveedores de Servicios ”
1021	Firmas Externas Que Obtienen Información de Empresa X Deben Hacerla Disponible	4.02.02.15	“ Información Recopilada Externamente ”
1022	Responsabilidades de Seguridad de Terceros en Conexiones en Tiempo Real	4.02.01.12	“ Responsabilidades de Terceros en la Seguridad Informática ”
1023	Definición Clara de las Responsabilidades de Terceros en la Seguridad Informática	4.02.02.16	“ Responsabilidades de Terceros en la Seguridad Informática ”
1024	Terminación de Contratos Externos por Violaciones a la Seguridad	4.03.01.09.	“ Aprobación de Contratos Externos ”
1025	Condición Financiera de Proveedores Críticos Debe Revisarse Anualmente	4.02.01.13	“ Condición Financiera de Proveedores Importantes ”
1026	Evitar Conflictos de Interes Reales y Aparentes	6.01.04.14	“ Conflictos de Intereses ”
1027	Investigadores Deben Divulgar Patrocinantes y Todos los Conflictos Potenciales	8.07.06.54	“ Investigación Pública ”
1028	Trabajadores No Pueden Tener Relaciones Románticas con Personal de la Competencia	6.01.04.15	“ Relaciones Personales con la Competencia ”
1029	Medidas Disciplinarias por No Cumplimiento de Seguridad Informática	6.03.05.01	“ Consecuencias de Incumplimiento ”
1030	Medidas Disciplinarias por Distintas Violaciones de Seguridad Informática	6.03.05.02	“ Consecuencias de las Violaciones ”
1031	Divulgación No Autorizada de la Información y Pérdida de Opciones en Valores	6.03.05.03	“ Pérdida de Opciones en Valores ”
1032	Violaciones de Seguridad que Exigen Despido Inmediato	6.03.05.04	“ Despidos Inmediatos ”
1033	Notificación y Manejo de Empleados Que Van a Trabajar con la Competencia	6.01.04.16	“ Renuncia de Empleados por la Competencia ”
1034	Notificación Inmediata a Empleados de Cese de Relación Laboral	6.01.04.17	“ Notificación de Cese de Empleo ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1035	Informe a Contratistas y Proveedores de Cese de Trabajador	6.01.04.18	“Notificación a Terceros de Cese de Trabajador”
1036	Manejo de Despidos de Trabajadores de Computación	6.01.04.19	“Manejo de Despidos”
1037	Escolta de Seguridad para Trabajadores Despedidos	6.01.04.20	“Escolta para Trabajadores Despedidos”
1038	Remoción de Información al Terminar Empleo	6.01.04.21	“Retención de Información al Terminar Empleo”
1039	Devolución de Información por Contratistas, Consultores y Empleados Temporales	4.02.02.17	“Devolución de la Información por el Personal Contratado”
1040	Devolución de Propiedad de la Empresa X al Momento de Separación de la Empresa X	6.01.04.22	“Devolución de Propiedad al Cesar Empleo”
1041	Responsabilidad por Tomar Acción Como Respuesta a Cese de Trabajador	12.02.01.02	“Responsabilidad por Cese de Trabajador”
1042	Los Empleados Despedidos No Pueden Volverse a Emplear o Utilizar Como Consultores	6.01.02.05	“Re-empleo de Empleados Despedidos”
1043	Período de Prueba para Trabajadores Nuevos o Re-empleados	6.01.02.06	“Periodo de Prueba Para Trabajadores Nuevos”
1044	Obligatorio Permiso No Remunerado Durante Investigaciones Extensas	6.03.01.25	“Investigaciones Prolongadas”
1045	Firma Anual de Convenio de Cumplimiento de Políticas de Seguridad	6.02.01.15	“Convenio de Cumplimiento”
1046	Cuándo Buscar Restitución	3.01.01.08	“Infracción de la Ley”
1047	Intervención Humana Requerida en Decisiones Importantes	10.02.02.14	“Intervención Humana en Procesos Asistidos por el Computador”
1048	Dependencia de una Sola Persona para Pericia en Sistemas Importantes	8.01.01.12	“Pericia en Sistemas”
1049	Obligatorios Cinco Días Consecutivos de Vacaciones Cada Año	6.01.04.23	“Días Consecutivos de Vacaciones”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1050	Impacto de Segundo Trabajo sobre la Objetividad y la Competencia con el Patrono	6.01.04.24	“ Segundos Trabajos ”
1051	Segundos Trabajos Deben Ser Divulgados en Entrevista Inicial o al Tomarlos	6.01.04.25	“ Divulgación de Segundos Trabajos ”
1052	Rotación Periódica del Trabajo para los Trabajadores del Area de Computación	8.01.04.01	“ Rotación de Trabajo ”
1053	Fianzas para Personas En Puestos de Confianza en Computación	6.01.02.07	“ Fianzas de Trabajadores ”
1054	Calificación del Personal Que Trabaja en los Proyectos Más Confidenciales de la Empresa X	6.01.02.08	“ Trabajo en Proyectos Sensibles ”
1055	Trabajadores de Confianza No Pueden Ser Clientes de la Empresa X	6.01.04.26	“ Trabajadores Como Clientes ”
1056	Obligación de Reportar Cambios en Situación Que Afecten la Eligibilidad para Ciertos Cargos	6.01.04.27	“ Informe de Cambios en Situación ”
1057	Transferencia de Ciertos Trabajadores a Cargos Con Menor Exposición	6.01.04.28	“ Transferencias de Trabajadores ”
1058	Uso de Convictos Violentos y la Seguridad en Sitio de Trabajo	6.01.02.09	“ Convictos Violentos ”
1059	Uso de Convictos en Cargos de Confianza en el Area de Computación	6.01.02.10	“ Cargos de Confianza en el Area de Computación ”
1060	Revisión de Antecedentes para Cargos de Confianza en Computación	6.01.02.11	“ Revisión de Antecedentes ”
1061	Personal Debe Pasar Revisión de Antecedentes Antes de Acceder a Información Privada	6.01.02.13	“ Acceso a Información Privada ”
1062	Acceso a Información Sensible de Productos Requiere Revisión de Antecedentes	6.01.02.14	“ Información Sensible de Productos ”
1063	Huellas Digitales de Empleados con Acceso a Información Confidencial	6.01.02.15	“ Huellas Digitales de Empleados ”
1064	Pruebas de Honestidad y Estabilidad Emocional para Trabajadores en el Area de Computación	6.01.02.16	“ Pruebas de Honestidad y Estabilidad Emocional ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1065	Prohibidos Extranjeros en Trabajos con Sistemas Informáticos	6.01.02.18	“Extranjeros”
1066	Aumentos Significativos e Inexplicados de Riqueza Deben Ser Investigados	6.01.02.20	“Aumento Significativo de Riqueza”
1067	Procedimientos Adecuados de Resolución de Quejas	6.01.04.29	“Resolución de Quejas”
1068	Servicios Confidenciales Gratuitos de Orientación para los Trabajadores	6.01.04.30	“Orientación Confidencial”
1069	Sitios de Trabajo Libres de Drogas y Alcohol	6.01.04.31	“Drogas y Alcohol”
1070	Convenios de No Competir Obligatorios para Empleados	6.01.03.05	“Convenios de No Competencia”
1071	Adiestramiento Técnico y Educación Continua del Personal de Sistemas Informáticos	6.02.01.16	“Adiestramiento Técnico y Educación Continua”
1072	Comité Gerencial de la Seguridad Informática	4.01.01.02	“Comité de Gestión de Seguridad Informática”
1073	Propiedad de la Información y Responsabilidades de la Gerencia	5.01.01.06	“Propiedad de la Información”
1074	Planes Divisionales para el Cumplimiento de la Seguridad Informática	12.02.01.03	“Planes Divisionales para el Cumplimiento de la Seguridad Informática”
1075	Asignación de la Responsabilidad de los Controles Sobre los Activos Informáticos	5.01.01.07	“Control de los Activos Informáticos”
1076	Implantación de Controles Consistente Con Normas de Debido Cuidado	12.02.01.04	“Normas de Implementación de Controles”
1077	Manejo de Variaciones Respecto de Prácticas de Control Generalmente Aceptadas	12.02.01.05	“Variaciones Respecto de Prácticas de Control Generalmente Aceptadas”
1078	Seguridad Informática es Tarea de Cada Trabajador	6.02.01.17	“Responsabilidad en la Seguridad Informática”
1079	Responsabilidad Centralizada de la Seguridad Informática	4.01.03.09	“Seguridad Informática Centralizada”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1080	Bosquejo de Tareas Realizadas por el Departamento de Seguridad Informática	4.01.03.10	“Responsabilidades del Departamento de Seguridad Informática”
1081	Tareas Específicas Realizadas por el Departamento de Seguridad Informática	4.01.03.11	“Tareas del Departamento de Seguridad Informática”
1082	La Misión del Departamento de Seguridad Informática Apoya las Metas de la Empresa X	4.01.03.12	“Misión del Departamento de Seguridad Informática”
1083	Autoridad para Crear Normas y Procedimientos de Seguridad Informática	4.01.03.13	“Normas y Procedimientos de Seguridad Informática”
1084	Obligatorio Proceso de Planificación Anual de Seguridad Informática	4.01.03.14	“Planes de Seguridad Informática”
1085	Evaluación Anual de Riesgo en Seguridad Informática en Toda la Organización	12.02.02.03	“Evaluación de Riesgo de Seguridad Informática en Toda la Organización”
1086	Evaluaciones de Riesgo Realizadas por los Sistemas Gerenciales de las Unidades de la Organizacion	12.02.01.06	“Evaluaciones de Riesgo de los Sistemas”
1087	Obligatorio Manual de Seguridad Informática Actualizado	4.01.03.15	“Manual de Seguridad Informática”
1088	Participación del Departamento Interno de Seguridad Informática	8.01.03.11	“Resolución de Problemas de Seguridad Informática”
1089	Revisión Pronta de Facturas por Servicios Computacionales y Comunicacionales	8.01.01.13	“Facturas por Servicios Computacionales y Comunicacionales”
1090	Quiénes Deben Cumplir Los Requisitos de Seguridad Informática	4.02.02.18	“Cumplimiento de Seguridad Informática”
1091	Administrador de Seguridad Designado para Todos los Sistemas Multiusuario	5.01.01.08	“Administrador de Seguridad Designado”
1092	Administrador de Seguridad Suplente Debe Ser Designado y Adiestrado	5.01.01.09	“Administradores de Seguridad Suplentes”
1093	Cada Departamento Debe Tener un Enlace con Seguridad Informática	4.01.03.16	“Enlaces de Seguridad Informática”
1094	Revisión Anual de Secretos Empresariales, Derechos de Autor, Etc., por Departamento Legal	12.01.02.22	“Revisión de Secretos Empresariales y Derechos de Autor”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1095	Revisión de Auditoría Interna de los Controles de los Sistemas Informáticos	12.03.01.02	“Revisión de los Controles de los Sistemas Informáticos — Interno”
1096	Auditoría Interna Realiza Verificación de Cumplimiento de Seguridad Informática	12.03.01.03	“Verificación de Cumplimiento de Seguridad Informática”
1097	Revisión Periódica Independiente de los Controles de la Seguridad Informática	4.01.07.02	“Revisión de los Controles de los Sistemas Informáticos — Independiente”
1098	Responsabilidad en Seguridad Informática Incluida en Descripción del Cargo	6.01.01.01	“Descripción del Cargo”
1099	Seguridad Informática Considerada en las Evaluaciones de Desempeño	6.01.01.02	“Evaluaciones de Desempeño”
1100	Separación de Tareas y Control Sobre los Activos de la Empresa X	8.01.04.02	“Separación de Tareas”
1101	Sistemas Construidos de Manera Tal Que los Errores y las Manipulaciones Salen a la Luz	10.02.02.15	“Erros y Manipulación de Registros”
1102	Instrucciones Específicas Respecto de la Separación de Tareas	8.01.04.03	“Instrucciones Sobre la Separación de Tareas”
1103	Responsabilidades en el Manejo de Incidentes	8.01.03.12	“Responsabilidades en el Manejo de Incidentes”
1104	Inventario Alto de Activos Informáticos	5.01.01.10	“Inventario de Activos — Información”
1105	Criterios para Asignar Propiedad de la Información	4.01.03.17	“Asignación de la Propiedad de la Información”
1106	El Departamento de Sistemas Informáticos No Debe Ser Propietario de Información	4.01.03.18	“Responsabilidad de la Propiedad en el Departamento de Sistemas Informáticos”
1107	Custodio Designado Obligatorio para Todos los Tipos Importantes de Información	4.01.03.20	“Custodio de la Información”
1108	Responsabilidades de Seguridad de los Custodios de la Información	4.01.03.21	“Responsabilidades del Custodio de la Información”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1109	Responsabilidades de Seguridad de los Usuarios de la Información	4.01.03.22	“Responsabilidades del Usuario de la Información”
1110	Proceso para otorgar Acceso a la Información de la Empresa X	9.01.01.34	“Otorgamiento de Acceso a la Información de la Organización”
1111	Tareas Restringidas en la Delegación de la Propiedad de la Información	4.01.03.23	“Delegación de la Propiedad de la Información”
1112	Control de Acceso Físico Hacia las Areas Que Contienen Información Sensible	7.01.02.01	“Control de Acceso Físico a la Información Sensible”
1113	Cuando las Oficinas Están Vacías, las Puertas Deben Estar Bajo Llave	7.01.02.02	“Cierre de Oficinas Personales”
1114	Sistemas Multiusuario de Computación o Comunicación en Salones Cerrados	7.01.03.02	“Aseguramiento de los Sistemas de Computación o Comunicación”
1115	Guardias o Recepcionistas para Areas Que Contienen Información Confidencial	7.01.01.01	“Acceso Físico para Terceros”
1116	Los Distintivos Deben Llevarse en Sitio Visible en las Instalaciones de la Empresa X	7.01.02.03	“Distintivos de Identificación”
1117	Distintivos Temporales para Trabajadores Que Olvidan sus Distintivos	7.01.02.04	“Distintivos Temporales”
1118	Reporte de Distintivos Perdidos/Robados y Tarjetas de Acceso	6.03.01.26	“Distintivos de Acceso Extraviados”
1119	Cada Individuo Debe Tener Su Distintivo Listo en Cada Puerta Controlada	7.01.02.05	“Acceso Controlado con Distintivos”
1120	No Se Permite Usar Distintivos de Otros en Puertas Controladas	7.01.02.06	“Distintivos de Acceso Compartidos”
1121	Puertas de Par en Par en Centro de Computación Requieren Presencia de Guardia	7.01.03.03	“Aseguramiento de Puertas Abiertas de Par en Par en Centros de Computación”
1122	Prohibido Probar Control de Acceso Físico	7.01.02.08	“Intentos No Autorizados de Acceso Físico”
1123	Prohibido Trabajar Solo En Areas Restringidas	7.01.04.03	“Trabajo en Areas Restringidas”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1124	Trabajo en Areas Restringidas Sólo Durante Horas Hábiles	7.01.04.04	“Horario de Areas Restringidas”
1125	Seguridad Física o Cifrado Necesario para Toda Información Confidencial	8.06.03.24	“Seguridad de la Información Sensible”
1126	Pases de Propiedad para Remover Equipos de Computación y de Comunicaciones	7.03.02.01	“Pases de Propiedad”
1127	Medios de Almacenamiento Deben Tener un Pase Autorizado Para Salir de las Instalaciones	7.03.02.03	“Traslado de Medios”
1128	Trabajadores Deben Mostrar Contenido de su Equipaje al Salir de las Instalaciones	7.01.02.09	“Inspección de Bolsos”
1129	Entrega de Gabinetes Metálicos con Cerradura al Personal Que Trabaja en Casa	9.08.02.07	“Gabinetes Metálicos con Cerradura”
1130	Registros de Control de Acceso al Edificio	7.01.02.10	“Registros del Sistema de Control de Acceso”
1131	Cambios de Códigos de Control de Acceso Físico del Trabajador Cesado	7.01.02.11	“Acceso Físico de Trabajadores Cesados”
1132	Derechos de Acceso a Areas Restringidas Deben Ser Revocados al Cesar Relación Laboral	7.01.02.12	“Acceso de Trabajadores Cesados a Areas Restringidas”
1133	Lista de Aquellos Que Pueden Permitir Acceso Físico	7.01.02.13	“Lista de Otorgantes de Acceso Físico”
1134	Reportes Periódicos de Distintivos de Identificación Emitidos a los Jefes de Departamento	7.01.02.14	“Reportes de Distintivos de Identificación”
1135	Proceso de Identificación y Firma para Todos los Visitantes	7.01.02.15	“Identificación de Visitantes”
1136	Escoltas para Todos los Visitantes	7.01.02.16	“Escolta de Visitantes”
1137	Escoltas Obligatorios Para Todos Los Visitantes en Horas No Hábiles	7.01.02.17	“Escoltas Obligatorios para Todos los Visitantes en Horas No Hábiles”
1138	Supervisión de Terceros en Areas Que Contienen Información Confidencial	7.01.02.18	“Supervisión de Terceros”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1139	Individuos Sin Distintivos de Identificación Deben Ser Atendidos	7.01.02.19	“Personas Sin Distintivos de Identificación”
1140	Remoción de Distintivos Despues de Salir de las Instalaciones de la Empresa X	6.01.04.32	“Remoción de Distintivos de Identificación”
1141	Manejo de Distintivos Cuando Los Trabajadores No Están en las Instalaciones de la Empresa X	6.01.04.33	“Aseguramiento de los Distintivos”
1142	Visitantes sin Escolta en Areas Restringidas Deben Ser Atendidos	7.01.02.20	“Visitantes sin Escolta”
1143	No Se Permiten Visitantes en Centro de Datos en el Departamento de Sistemas Informáticos	7.01.02.21	“Visitantes al Centro de Datos y al Departamento de Sistemas Informáticos”
1144	Todas las Estaciones de Trabajo Deben Utilizar Llaves Metálicas para Controlar el Acceso	7.02.01.09	“Llaves de las Estaciones de Trabajo”
1145	Puertas de los Gabinetes de los Equipos de Computación y Comunicaciones Deben Estar Bajo Llave	7.02.01.10	“Puertas de Gabinetes de Equipos”
1146	Sistemas Comerciales y Financieros en Internet Deben Estar Físicamente Aislados	7.02.01.11	“Sistemas Comerciales y Financieros en Internet”
1147	Aislamiento de Equipos Entre Empresa X y Sistemas de Terceros	7.02.01.12	“Aislamiento de Equipos”
1148	Medidas de Seguridad Física para Sistemas de Computación y Comunicación	7.01.02.22	“Acceso a Sistemas de Computación y Comunicación”
1149	Actividades Críticas o Sensibles Permitidas Solamente en Areas Físicamente Seguras	7.01.02.23	“Aseguramiento de Actividades de Manejo de Información Sensible o Crítica”
1150	El Centro de Computación es un Taller Cerrado	7.01.02.24	“Acceso al Centro de Computación”
1151	Lista de Acceso del Personal Autorizado al Centro de Computación Revisada Trimestralmente	7.01.02.25	“Acceso del Personal al Centro de Computación”
1152	Centralización de Todos los Dispositivos Críticos de Voz y Datos en Red	8.05.01.48	“Dispositivos Críticos de Voz y Datos en Red”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1153	Acceso restringido a Cintas Magnéticas, Discos y Librerías de Documentación	7.01.02.26	“ Acceso a Librerías de Medios ”
1154	Areas de Equipos Vacías Deben Estar Bajo Llave y Revisarse Periódicamente	7.01.04.05	“ Areas de Equipos Vacías ”
1155	Areas de Equipos de Comunicaciones Cerradas y Acceso Escoltado	7.01.04.06	“ Areas de Equipos de Comunicaciones ”
1156	Prohibidas las Giras Turísticas en las Instalaciones de Computación	7.01.02.27	“ Visitas a las Instalaciones de Computación ”
1157	Prohibidas las Cámaras y Equipos de Grabación de Audio y Video	7.01.04.07	“ Equipos de Grabación de Audio o Video ”
1158	Impresoras, Copiadoras y Faxes Prohibidos en Areas de Información Secreta	7.01.03.04	“ Equipos en Areas de Información Secreta ”
1159	Ubicación de Nuevos Centros de Computación o Comunicaciones	7.02.01.13	“ Ubicaciones de Centros de Computación ”
1160	Suministros Básicos Redundantes	7.02.02.02	“ Proveedores Redundantes de Suministros Básicos ”
1161	Construcción Adecuada de Centros de Computación o Comunicaciones	7.02.01.14	“ Construcción del Centro de Computación ”
1162	Ubicación del Centro de Computación o Comunicaciones Dentro de un Edificio	7.01.01.03	“ Ubicación del Centro de Computación y Comunicaciones ”
1163	Ubicación del Equipo de Computación Debe Poseer Precauciones Contra Daños por Agua	7.02.01.15	“ Precauciones ante Daños por Agua ”
1164	Area Intermedia Obligatoria para Restringir Acceso al Centro de Computación	7.01.05.01	“ Entregas al Centro de Computación ”
1165	No Debe Hacer Avisos Indicando Ubicación del Centro de Computación o Comunicaciones	7.01.03.05	“ Señalización de Centros de Computación y Comunicaciones ”
1166	Resistencia al Fuego en Centros de Computación y Aberturas con Autocierre	7.01.01.04	“ Resistencia al Fuego de Centros de Computación ”
1167	Centros y Puertas Resistentes a Entradas Forzadas	7.01.01.05	“ Solidez de las Puertas de Centros de Computación ”

Tabla O-1: Indice de Nuevos Nombres de las Políticas (Continued)

Número Política Anterior	Título Versión 8	Número Política Actual	Título Versión 9
1168	Centros de Computación y Puertas Automáticas	7.01.01.06	“Cierre de Puertas en Centros de Computación”
1169	Puertas Adicionales de Acceso al Centro de Computación Deben Tener Barras de Protección y Alarmas	7.01.01.07	“Puertas Adicionales de Acceso al Centro de Computación”
1170	Seguimiento de Equipos Asistido por Computador	5.01.01.11	“Seguimiento de Equipos”
1171	Marcar Equipos de Sistemas Informáticos con Códigos de Identificación	5.01.01.12	“Códigos de Identificación de los Equipos”
1172	Prohibido Traslado de Equipos de Microcomputadores sin Permiso	8.07.05.59	“Traslado de Equipos de Computación de Oficinas”
1173	Alarmas de Incendio, Agua, o Entradas de Intrusos Provocan Acción Inmediata	7.02.01.16	“Alarmas del Centro de Computación”
1174	Posicionamiento de las Pantallas de los Computadores con Respecto a las Ventanas	8.07.05.60	“Posiciones de las Pantallas de los Computadores”
1175	Protección Contra la Radiación (Emanación) Electromagnética para Sistemas Secretos	8.07.05.61	“Protección Contra la Radiación Electromagnética”



ACERCA DEL AUTOR



Desde sus oficinas de la Bahía de San Francisco, Charles Cresson Wood se desempeña como consultor independiente de seguridad informática, investigador y escritor. Como parte de su rutina, prepara y revisa estándares, arquitecturas, políticas, códigos de conducta, procedimientos, presupuestos, planes de acción, declaraciones de misión, perfiles y varios otros ítemes de la infraestructura necesaria para apoyar la seguridad informática. También realiza evaluaciones de riesgo y diseña soluciones de seguridad informática adaptadas a las necesidades del cliente.

En el campo a tiempo completo desde 1979, el Sr. Wood se ha ocupado de la consultoría en gestión de seguridad computarizada de SRI International (antiguamente conocido como el Instituto de Investigación de Stanford) y principal consultor en seguridad de comunicaciones de datos del Bank of America. Ha realizado trabajo de consultoría en seguridad informática para más de 120 organizaciones, muchas de ellas empresas mencionadas en Fortune 500. Sus proyectos de consultoría le han llevado a Australia, Austria, Bélgica, Brasil, Canadá, Inglaterra, Finlandia, Francia, Holanda, Irlanda, Italia, Japón, Noruega, Portugal, Arabia Saudí, África del Sur y Suecia.

El Sr. Wood ha efectuado más de 125 presentaciones sobre seguridad informática en distintas conferencias; siendo en muchos casos, el presentador oficial de las mismas. Sus palabras han sido citadas en calidad de experto en publicaciones importantes, tales como Business Week, Computerworld, Information Week, LA Times, PC Week, The Wall Street Journal y la revista Time. En 1996 recibió el Galardón por Logros que otorga el Instituto de Seguridad Computarizada (San Francisco) por “dedicación sincera a la profesión de seguridad informática”.

El Sr. Wood es Editor Principal en Norteamérica de las revistas técnicas Computers & Security y Computer Fraud and Security Bulletin. Durante los últimos seis años ha escrito una columna sobre políticas de seguridad informática para Computer Security Alert. Ha publicado más de 225 artículos técnicos y cinco otros libros sobre la seguridad informática. Su libro más vendido se titula *Políticas de Seguridad Informática - Mejores Prácticas Internacionales*. El trabajo del Sr. Wood ha sido o está siendo traducido a varias lenguas, entre ellas el portugués brasileño, finlandés, francés, japonés, hebreo, portugués, castellano y sueco.

El Sr. Wood posee un MBA en sistemas informáticos financieros y una licenciatura en contabilidad, ambos títulos conferidos por la Facultad Wharton de la Universidad de Pensilvania. También posee un título de ingeniero en ciencias de la computación otorgado por la Facultad Moore de Ingeniería de la misma universidad (lugar de nacimiento de ENIAC, la primera computadora electrónica del mundo). Además de ser Contador Público Certificado (CPA), el Sr. Wood es Auditor Certificado en Sistemas Informáticos (CISA) y Profesional Certificado en la Seguridad de Sistemas Informáticos (CISSP).

Otras Publicaciones de Charles Cresson Wood

Cómo Entender Roles y Responsabilidades en Seguridad Informática (PentaSafe, Houston, Texas, USA, 2001)

Las Mejores Prácticas en la Seguridad Comercial en Internet (PentaSafe, Houston, Texas, USA, 1998)

Cómo Manejar la Seguridad del Comercio Electrónico en Internet: Riesgos, Controles y Guía de Productos (PentaSafe, Houston, Texas, USA, 1996)

Gestión Eficaz de la Seguridad Informática (Elsevier Science Publishers, Oxford, England, 1991)

Seguridad Computarizada: Una Lista Completa de Verificación de los Controles (John Wiley and Sons, New York, New York, USA 1987)



