NORMAS Y ESTÁNDARES
PARA LA ADMINISTRACIÓN PÚBLICA

Seguridad

gobiernoelectrónico
REPÚBLICA DOMINICANA

OPTIC
Oficina Presidencial de Tecnologías de la Información y Comunicación

Conceptos Generales

QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad institucional, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características:

a) **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
b) **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que

abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la organización.

POR QUÉ ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN

La información, los sistemas y las redes que brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen institucional.

Las organizaciones, sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

CÓMO ESTABLECER LOS REQUERIMIENTOS DE SEGURIDAD

Es esencial que una organización identifique sus requerimientos de seguridad. Existen tres recursos principales para lograrlo.

El primer recurso consiste en evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.

El segundo recurso está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.

El tercer recurso es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

EVALUACIÓN DE LOS RIESGOS EN MATERIA DE SEGURIDAD

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Las erogaciones derivadas de la satisfacción de las necesidades de control deben ser equilibradas con respecto al impacto potencial de las fallas de seguridad en los negocios. Las técnicas de evaluación de riesgos pueden aplicarse a toda la organización, o sólo a partes de la misma, así como a los sistemas de información individuales, componentes de sistemas o servicios específicos cuando esto resulte factible, viable y provechoso.

La evaluación de riesgos es una consideración sistemática de los siguientes puntos;

a) impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos;
b) probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominantes, y los controles actualmente implementados.

Los resultados de esta evaluación ayudarán a orientar ya determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos. Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse a cabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante llevar a cabo revisiones periódicas de los riesgos de seguridad y de los controles implementados a fin de:

a) reflejar los cambios en los requerimientos y prioridades de la empresa;
b) considerar nuevas amenazas y vulnerabilidades;
c) corroborar que los controles siguen siendo eficaces y apropiados.

Las revisiones deben llevarse a cabo con diferentes niveles de profundidad según los resultados de evaluaciones anteriores y los niveles variables de riesgo que la gerencia está dispuesta a aceptar. Frecuentemente, las evaluaciones de riesgos se realizan primero en un nivel alto, a fin de priorizar recursos en áreas de alto riesgo, y posteriormente en un nivel más detallado, con el objeto de abordar riesgos específicos.

PUNTO DE PARTIDA PARA LA SEGURIDAD DE LA INFORMACIÓN

Algunos controles pueden considerarse como principios rectores que proporcionan un buen punto de partida para la implementación de la seguridad de la información. Están basados en requisitos legales fundamentales, o bien se consideran como práctica recomendada de uso frecuente concerniente a la seguridad de la información.

Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:

a) protección de datos y confidencialidad de la información personal
b) protección de registros y documentos de la organización ;
c) derechos de propiedad intelectual ;

Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información comprenden:

a) documentación de la política de seguridad de la información;
b) asignación de responsabilidades en materia de seguridad de la información;
c) instrucción y entrenamiento en materia de seguridad de la información;
d) comunicación de incidentes relativos a la seguridad;
e) administración de la continuidad de la empresa;

Estos controles son aplicables a la mayoría de las organizaciones y en la mayoría de los ambientes. No todos los controles aquí descritos están desarrollados en este documento. Se debe ver este documento como la primera de múltiples ediciones a ser desarrolladas. El objetivo final es lograr obtener aplicaciones de todos los puntos de la ISO 17799 y la ISO 27001.

Se debe observar que aunque todos los controles mencionados en este documento son importantes, la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que

afronta la institución. Por ello, si bien el enfoque delineado precedentemente se considera un buen punto de partida, éste no pretende reemplazar la selección de controles que se realiza sobre la base de una evaluación de riesgos.

DESARROLLO DE LINEAMIENTOS PROPIOS

Este conjunto politicas puedem ser considerado como un punto de partida para el desarrollo de lineamientos específicos, aplicables a cada institucion. No todos los lineamientos y controles de este código de práctica resultarán aplicables. Más aún, es probable que deban agregarse controles que no están incluidos en este documento. Ante esta situación puede resultar útil retener referencias cruzadas que faciliten la realización de pruebas de cumplimiento por parte de auditores y socios.

Alcance

Este documento brinda recomendaciones para la gestión de la seguridad de la información que han de ser aplicadas por los responsables de iniciar, implementar o mantener la seguridad en sus instituciones. Su propósito es proveer de una base común para el desarrollo de estándares de seguridad en sector gobierno de la República Dominicana; y una práctica efectiva de la administración de la misma, brindando asimismo, confianza en las relaciones llevadas a cabo entre las instituciones.

Términos y Definiciones

SEGURIDAD DE LA INFORMACIÓN

La preservación de la confidencialidad, integridad y disponibilidad de la información.

EVALUACIÓN DE RIESGOS

La evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

ADMINISTRACIÓN DE RIESGOS

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.

Políticas de Seguridad

AREAS SEGURAS

I. Perímetro de Seguridad Física

1. Acceso Físico para Terceros

Política:

El acceso de visitantes o terceros a las oficinas de la Institución, 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.

Política Dirigida a: Gerencia

2. Plan de Seguridad Física

Política:

Todo centro de datos de la Institución 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.

Política Dirigida a: Gerencia

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.

Política Dirigida a: Gerencia y personal técnico

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.

Política Dirigida a: Gerencia y personal técnico

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, especial-mente 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.

Política Dirigida a: Gerencia

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.

Política Dirigida a: Gerencia

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 específica 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. La alarma puede también avisar a otros que puede haber un incendio o cualquier otro problema que necesita atención inmediata.

Política Dirigida a: Personal técnico

II. Aseguramiento de Oficinas, Salones e Instalaciones

1. 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.
Política Dirigida a: Personal técnico

2. 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.
Política Dirigida a: Personal técnico

3. 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 Institución 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 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.
Política Dirigida a: Gerencia y personal técnico

4. 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 de 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.
Política Dirigida a: Gerencia

SEGURIDAD DE LOS EQUIPOS

I. Ubicación y Protección de los Equipos

1. Ubicación de Sistemas de Computación de Producción

Política:
Todos los sistemas computarizados de producción incluyendo, sin limitantes, servidores, cortafuegos, concentradores, enrutadores 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.
Política Dirigida a: Usuarios finales

2. 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 Institución.
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 políti-

ca asume que la palabra "crítica" se definió en otra política.
Política Dirigida a: Gerencia y personal técnico

3. 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 especificas 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".
Política Dirigida a: Personal técnico

4. 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 Institución. 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.
Política Dirigida a: Personal técnico

5. Infraestructura de Respaldo para Centro de Datos
Política:
La Institución 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 ser-

vicios 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.
Política Dirigida a: Personal técnico

6. Sistemas de Computación Pertenecientes a Trabajadores

Política:
Los trabajadores no deben traer a las instalaciones de la Institución 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 Institución.
Política Dirigida a: Usuarios finales y personal técnico

7. Llaves de las Estaciones de Trabajo

Política:
Todas las estaciones de trabajo de escritorio de la Institución 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.
Política Dirigida a: Usuarios finales

8. 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 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 rejas de metal o la colocación de paredes normales dentro del centro de datos en el mismo formato en que se encuentra esta política.

Política Dirigida a: Personal técnico

9. 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 segrega 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 reinicializar 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.

Política Dirigida a: Personal técnico

10. Aislamiento de Equipos

Política:

Los equipos de computación y comunicaciones manejados por personal de la Institución, 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 Institución. El acceso físico puede permitir que personas no autorizadas reinicialicen 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 data, entonces los terceros deben estar en el mismo salón donde está ubicado el equipo que maneja la Institución. 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 Institución 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 Institución pueden ser un prerrequisito al uso de herramientas de administración de redes remotas y para establecer operaciones nocturnas.
Política Dirigida a: Personal técnico

11. Ubicaciones de Centros de Computación
Política:
Todos los centros nuevos de computación o de comunicación de la Institución, 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.
Política Dirigida a: Gerencia y personal técnico

12. Construcción del Centro de Computación
Política:
Los centros de computación y comunicación de la Institución, 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.
Política Dirigida a: Gerencia y personal técnico

13. Precauciones ante Daños por Agua
Política:
Todos los locales de la Institución 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.
Política Dirigida a: Personal técnico

14. Alarmas del Centro de Computación

Política:
Todos los centros de computación de la Institución 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.
Política Dirigida a: Personal técnico

II. 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 potencias eléctricas 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, súper-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.
Política Dirigida a: Todos

2. Proveedores Redundantes de Suministros Básicos

Política:
Todos los nuevos centros de computación y de comunicaciones de la Institución 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.
Política Dirigida a: Gerencia y personal técnico

III. 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.
Política Dirigida a: Todos

IV. 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 Institución 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.
Política Dirigida a: Usuarios finales y personal técnico

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 producción". 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Usuarios finales y personal técnico

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 Institución 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.
Política Dirigida a: Personal técnico

5. Modificaciones a Computadores
Política:
Los equipos de computación suministrados por la Institución no deben alterarse de ninguna manera ni añadírseles 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 Institución. 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 asignado a un usuario es el equipo que será devuelto cuando el usuario abandone la Institución. 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.
Política Dirigida a: Usuarios finales

III. 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 Institución 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 Institución. 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 cuando el equipo está dentro de las instalaciones de la Institución. 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.
Política Dirigida a: Todos

IV. 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 Institución, 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 po-

líticas que establecen que la compra de equipos de sistemas informáticos debe estar centralizada.
Política Dirigida a: Gerencia y personal técnico

2. Disposición de Información y Equipos
Política:
Los gerentes departamentales son responsables de la disposición de la propiedad sobrante que ya no se necesite 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.
Política Dirigida a: Gerencia

PROTECCIÓN CONTRA SOFTWARE MALICIOSO

I. 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 Institución.
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".
Política Dirigida a: Usuarios finales

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.

Política Dirigida a: Usuarios finales

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, más 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.

Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Todos

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 Institución 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 forzarse mediante el uso de software de gestión de licencias o software para controlar modificaciones en computadores personales.
Política Dirigida a: Usuarios finales y personal técnico

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 Institución.
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 Institución. 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 Institución 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.

Política Dirigida a: Usuarios finales

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 Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

8. Instalación de Software Antivirus

Política:

Debe estar instalado y habilitado software para verificar la presencia de virus en todos los cortafuegos de la Institución, 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 vi-

rus 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 eliminen menos se propagarán, se recomienda un chequeo de virus en todas las localidades especificadas.
Política Dirigida a: Personal técnico

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 Institución 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.
Política Dirigida a: Personal técnico

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 Institución, 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.
Política Dirigida a: Usuarios finales

11. Exploración de Software Descargado
Política:
Antes de descomprimir el software descargado de fuentes ajenas a la Institución, 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.
Política Dirigida a: Usuarios finales

12. Verificación de la Integridad del Sistema
Política:
Todos los computadores personales y los servidores de la Institución 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 Institución. 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.
Política Dirigida a: 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 po-

lítica 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.
Política Dirigida a: Usuarios finales

14. Software Antivirus Actual

Política:
Cada trabajador de la Institución 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 Institución 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 Institución 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales

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.

Política Dirigida a: Usuarios finales y personal técnico

17. Rastreo de Virus en Archivos de Respaldo

Política:

Antes de restaurar los archivos de los sistemas informáticos de la Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

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 Institución.

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.

Política Dirigida a: Usuarios finales y personal técnico

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.

Política Dirigida a: Usuarios finales

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 Institución, 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.

Política Dirigida a: Usuarios finales y personal técnico

21. Actualizaciones Automáticas de Software

Política:

No deben efectuarse actualizaciones automáticas de software en los computadores de la Institución a través del uso de la tecnología push, a menos que el software utilizado haya sido evaluado por un integrante autorizado del departamento de Sistema 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 ahorran 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 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 políti-

ca 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.
Política Dirigida a: Personal técnico

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 Institución 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
Política Dirigida a: Personal técnico

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 automatizado 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.
Política Dirigida a: Usuarios finales y personal técnico

24. Información Descargada

Política:
Todo software y archivos descargados de fuentes ajenas a la Institución, 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 soft-

ware, 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.
Política Dirigida a: Todos

MANTENIMIENTO

I. 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.
Política Dirigida a: 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 Institución.
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 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.
Política Dirigida a: 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 Institución.
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 computa-dores 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.
Política Dirigida a: Usuarios finales

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 Institución.
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 tele-trabajadores, para los que utilizan computadores personales y otros sistemas que hayan sido retirados de las instalaciones de la Institución. 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.
Política Dirigida a: Todos

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.
Política Dirigida a: Personal técnico

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 Institución.

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.

Política Dirigida a: Personal técnico

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 engorroso 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.

Política Dirigida a: Personal técnico

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".
Política Dirigida a: Usuarios finales y personal técnico

9. Revisión de la Información Respaldada
Política:
Todos los archivos y los mensajes almacenados en los sistemas de la Institución 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 Institución. 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Todos

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.
Política Dirigida a: Personal técnico

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 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Personal técnico

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 archivadas 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.
Política Dirigida a: Personal técnico

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 políti-

ca 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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
Política Dirigida a: 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: 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 medíos 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.
Política Dirigida a: Gerencia y personal técnico

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 Institución.
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.
Política Dirigida a: Personal técnico

II. REGISTROS DE OPERADORES

1. Registros de Operadores de Computadores

Política:

Todos los sistemas multiusuario de producción de la Institución 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.

Política Dirigida a: Personal técnico

2. Revisión de Registros de Operadores de Computadores

Política:

Todos los registros de los sistemas multiusuario de producción de la Institución 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.

Política Dirigida a: Gerencia y personal técnico

III. 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 proble-

mas, 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.
Política Dirigida a: Todos

CONTROLES DE LAS REDES

I. 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 Institución no puede permitir que exista ningún tipo de relación de confianza entre los computadores conectados a la red interna de la Institución.
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 Institución. 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.
Política Dirigida a: Personal técnico

2. Configuración de Seguridad
Política:
Los parámetros de configuración y de instalación de todos los servidores incorporados a la red de la Institución 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 Institución.
Política Dirigida a: Personal técnico

3. Interfaces a Redes Externas
Política:
Los diseñadores y desarrolladores de los sistemas de la Institución 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.
Política Dirigida a: Personal técnico

4. Revisión de Conexiones Remotas
Política:
La Institución 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 Institución 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 Institución. 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 Institución. 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 Institución pueden estar conectados a su red interna. De prevalecer otro enfoque en el entorno, entonces se puede modificar la política.
Política Dirigida a: Usuarios finales

5. Control de Tráfico en Internet
Política:
La Institución 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.
Política Dirigida a: Usuarios finales

6. Cookies
Política:
Antes de que se utilicen cookies y en cualquiera de los sitios web y comerciales de la Institución, 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 protec-

tora de la privacidad, sólo serán utilizados en caso de extrema necesidad. La organización debe divulgar el uso de dichas tecnologías encaso 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

8. Punto Central de Falla de la Red
Política:
La gerencia debe diseñar las redes de comunicaciones de la Institución 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.
Política Dirigida a: Personal técnico

9. Mútiples Operadoras Telefónicas

Política:

La gerencia debe diseñar los sistemas de comunicaciones de la Institución 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 "critica" está definida en otra política.

Política Dirigida a: Personal técnico

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 Institución 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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

12. Servicios de Protección de Mensajes en Red

Política:

Al suministrar el servicio de redes de computación, la Institución no debe suministrar servicios de protección de mensajería.

Comentario:

Esta política es para aquellos suscriptores que utilizan la red de la Institución y para terceros con los cuales la Institución 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 Institución 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.
Política Dirigida a: Usuarios finales

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 Institución, deben ser restringidas de tal manera que tanto los sistemas como los usuarios que no pertenezcan a la red interna de la Institución 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 Institución 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 Institución utiliza conexiones con redes externas.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Usuarios finales y personal técnico

18. Acceso del Administrador al Cortafuego de Internet

Política:

Todos los cortafuegos de la Institución 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 autentificación de usuario, por ejemplo, contraseñas dinámicas o biométricas, y no sólo las contraseñas fijas tradicionales.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

20. Servidores Públicos en Internet

Política:

Los servidores públicos en Internet se deben ubicar en subredes, aparte de las redes internas de la Institución, y a las cuales se haya restringido el paso del público mediante enrutadores 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 computa-dores 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.

Política Dirigida a: Personal técnico

21. Conexiones Discadas

Política:

Todas las líneas discadas entrantes, con conexión a las redes internas o a los sistemas informáticos de la Institución, 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 proba-

blemente 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 autentificación extendida de usuarios. La ventaja de utilizar técnicas de autentificación 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.

Política Dirigida a: Personal técnico

22. Conexiones a Redes Externas en Tiempo Real

Política:

Todas las conexiones entrantes en tiempo real a las redes internas de la Institución 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.

Política Dirigida a: Personal técnico

23. Configuración de Cortafuegos

Política:

Todos los cortafuegos de la Institución 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 ser-

vicios 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.
Política Dirigida a: Personal técnico

24. Computadores para Cortafuegos
Política:
Todos los cortafuegos utilizados para proteger la red interna de la Institución, 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 podrá 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

26. Conexiones a Internet
Política:
Todas las conexiones entre las redes internas de la Institución 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 utili-

zadas 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.
Política Dirigida a: Personal técnico

27. Sistemas de Directorios Compartidos

Política:
El uso de sistemas de directorios compartidos en cualquier computador de la Institución 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.
Política Dirigida a: Personal técnico

28. Conexiones en Red con Organizaciones Externas

Política:
La creación de una conexión directa entre los sistemas de la Institución 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 Institución, qué información sobre los sistemas de la Institución 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.
Política Dirigida a: Usuarios finales y personal técnico

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 Institución. 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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Personal técnico

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 autentificación 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 Institución.
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 restablecer un control centralizado a lo largo de la organización sobre Seguridad Informática.
Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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 Institución 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 Institución a riesgos no considerados con antelación. La Institución puede ser considerada responsable de fraudes cometidos con sus sistemas, o si éstos han sido utilizados por delincuentes para almacenar datos de tarjetas de créditos robadas. Esta política impide que el personal de la Institución ofrezca las instalaciones de la misma hasta que los riesgos y demás responsabilidades hayan sido identificados plenamente y aceptados por la alta gerencia.

Política Dirigida a: Usuarios finales y personal técnico

34. Números de Acceso a Computadores

Política:

La información relacionada con el acceso a los sistemas de computación y comunicacionales de la Institución, 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 Institución. 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 ínter-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.

Política Dirigida a: Usuarios finales y personal técnico

35. Cambio de Números Discados

Política:

Los números telefónicos de las comunicaciones de computación de la Institución 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 Institución. 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.

Política Dirigida a: Personal técnico

36. Conexiones Salientes

Política:

Todos los usuarios que hayan establecido conexiones salientes desde las oficinas de la Institución, deben tener autentificadas 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 fuera una vez entren en el sistema de la Institución. 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 autentificar 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 autentificar definitivamente a los usuarios, lo que a menudo requiere que el departamento de Seguridad Informática defi-

na con exactitud el significado de dichas palabras. La tecnología que respalda la autentificación definitiva puede variar en el tiempo sin que exista la necesidad de redactar nuevamente la política.
Política Dirigida a: Personal técnico

37. Modem por Cable

Política:
No debe ser utilizado ningún módem por cable para las comunicaciones comerciales de la Institución, 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 tele-trabajadores cuando se conectan a un computador a través de Internet.
Política Dirigida a: Usuarios finales y personal técnico

38. Configuración de Modem para Llamadas Discadas Entrantes

Política:
Los módem de acceso telefónico de la Institución 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.
Política Dirigida a: Personal técnico

39. Contraseñas para Conexión Telnet

Política:
Los usuarios no deben implantar conexiones Telnet en los computadores de la Institución utilizando contraseñas fijas tradicionales en Internet, a menos que dichas conexiones se establezcan utilizando contraseñas dinámicas u otro tipo de tecnología autorizada para la autentificación 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 Institución. 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 autentificación 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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Personal técnico

41. Acceso a Internet

Política:
Todos los accesos a Internet utilizando los computadores de las oficinas de la Institución deben ser enrutados a través del cortafuego.
Comentario:
Esta política impide que los usuarios eludan 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 Institución. La política se restringe a los computadores instalados en las oficinas de la Institución, debido a que los tele-trabajadores y usuarios de computadores portátiles no se pueden regir por esta política.
Política Dirigida a: Usuarios finales y personal técnico

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 Institución 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.
Política Dirigida a: Personal técnico

43. Directorios Modificables por el Público

Política:
Todos los directorios modificables públicamente presentes en los computadores conectados a Internet de la Institución deben ser revisados y borrados todas las noches.
Comentario:
Esta política impide que los computadores de la Institución 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 Institución 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 automati-

zados a través de comandos, por lo que la puesta en práctica de esta política no debe ser costosa.
Política Dirigida a: Personal técnico

44. Redes Inalámbricas
Política:
Las redes inalámbricas utilizadas en las trasmisiones de la Institución 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 Institución. 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 Institución. Las redes inalámbricas permiten que los adversarios ataquen los sistemas de la Institución 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.
Política Dirigida a: Personal técnico

45. Puertas de Enlace a Redes Inalámbricas
Política:
Las puertas de enlace a redes inalámbricas de la Institución 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.
Política Dirigida a: Personal técnico

46. Sistemas en Interface con Redes Externas
Política:
Todos los sistemas de la Institución 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 impedida 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.
Política Dirigida a: Personal técnico

47. Medidas de Seguridad de la Red
Política:
Las medidas de seguridad de las redes de los sistemas de producción de la Institución 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.
Política Dirigida a: Personal técnico

48. Dispositivos Críticos de Voz y Datos en Red
Política:
Todos los dispositivos comerciales críticos que soportan el sistema telefónico de la Institución, 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 enrutadores. 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 constituyen 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.
Política Dirigida a: Personal técnico

MANEJO Y SEGURIDAD DE MEDIOS DE ALMACENAMIENTO

I. Manejo de Medios de Computación Removibles

1. Discos Flexibles
Política:
Todos los discos flexibles utilizados en la Institución 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.
Política Dirigida a: Usuarios finales

2. Almacenamiento de Información de Clasificación Mixta

Política:

Los trabajadores de la Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

3. Borrado de Información Sensible

Política:

Cuando la información sensible de la Institución 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 sobre escritura. 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.

Política Dirigida a: Todos

INTERCAMBIO DE INFORMACIÓN Y SOFTWARE

I. Convenios de Intercambio de información y Software

1. Software Distribuido a Terceros

Política:

Todo software desarrollado por la Institución 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 Institución. 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 fun-

cione 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 Institución en su intento de probar en un tribunal el uso de los controles adecuados para mantener el software como secreto industrial.
Política Dirigida a: Personal técnico

2. Convenios de Software con Terceros
Política:
Todo software desarrollado por la Institución 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 Institución.
Comentario:
Esta política genera acuerdos por escrito en cuanto al uso autorizado del software desarrollado por la Institución previo a su distribución. Ello impedirá el robo de la propiedad intelectual de la Institución 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 Institución 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.
Política Dirigida a: Personal técnico

3. Convenios de Intercambio de Software y Datos
Política:
Los intercambios de software o información interna entre la Institución 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 Institución. 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. Esta política podría ser restringida para que sólo haga referencia a la información confidencial y a la privada.
Política Dirigida a: Gerencia y personal técnico

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 Institución 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 Institución 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 Institución, 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 contentivos de información sensible. También puede ser que los medios contengan un programa que recopile información acerca de la Institución, 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 Institución 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 Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

5. Contratos en Línea con Intercambio de Papel y Firmas

Política:

Cada vez que terceros acepten una oferta en línea de la Institución, 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 Institución 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.

Política Dirigida a: Gerencia y personal técnico

6. Validación de la Identidad de Terceros

Política:

Antes de que los trabajadores publiquen la información interna de la Institución, 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 originarios. El uso de sistemas de cifrado que incorporan rasgos de autentificación proporcionan vías alternas para confirman la identidad de los que intercambian correspondencia en Internet.
Política Dirigida a: Usuarios finales

II. 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.
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.
Política Dirigida a: Usuarios finales

2. 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 Institución, 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 Institución. Esta política puede ampliarse para incluir discos flexibles y otros medios de almacenamiento no cifrados.
Política Dirigida a: Usuarios finales y gerencia

3. Transferencia de Información Sensible

Política:
Todos los medios de almacenamiento de computación enviados desde la Institución 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 sobre escrita, 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 sobre escritura 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

Política Dirigida a: Todos

III. Seguridad del (Gobierno Electrónico)

1. Obtención de Información desde Archivos Cookie

Política:

La Institución 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 Institución 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 simple-mente determinar qué tipos existen, con la intención de conseguir un perfil que revele los sitios visitados por un cliente. Recopilar esta información sin obtener previamente el permiso por parte del cliente, puede constituir una violación de la privacidad. La política garantiza a los clientes que la Institución no se dedica a este tipo de prácticas.

Publicar una política como ésta en Internet no compromete a la Institución ya que en el futuro, si se desea recolectar esta información, se debería por lo menos informar a los usuarios.

Política Dirigida a: Usuarios finales

2. Clasificación de Contenido y Protección de la Privacidad

Política:

La Institución 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.

Política Dirigida a: Usuarios finales

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 Institución, 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 Institución 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.
Política Dirigida a: Personal técnico

4. Colocación de Clientes y Prospectos en Listas de Correos

Política:
La Institución 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.
Política Dirigida a: Usuarios finales

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 Institución.
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.
Política Dirigida a: Personal técnico

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 Institución, 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.
Política Dirigida a: Personal técnico

7. Confirmación de Cambio Solicitado por Cliente
Política:
Todo cambio iniciado por un cliente en cuanto a su relación con la Institución, 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 Institución. 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 Institución 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.
Política Dirigida a: Gerencia y personal técnico

8. Investigación de Errores
Política:
Los errores detectados por los clientes en los registros de la Institución 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 Institución. Dicha empresa establece un tiempo de respuesta para responder al cliente y comunicar a los trabajadores de la Institución 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 Institución 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.
Política Dirigida a: Todos

9. Seguridad de los Servidores Comerciales en Internet
Política:
Todos los servidores comerciales de Internet de la Institución, 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.
Política Dirigida a: Personal técnico

10. Servicio Nuevo o Mejorado

Política:
Los clientes que reciban servicios de computación o de comunicaciones de la Institución, 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 Institución. La política requiere el soporte de todos los servicios previamente disponibles. Esto no impide a la Institución 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 recibirlos. 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 Institución 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 Institución. Esto evitará que la Institución 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.
Política Dirigida a: Gerencia y personal técnico

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. "Software y Datos," y "Firmas Legales"
Política Dirigida a: Gerencia y personal técnico

12. Transacciones Internacionales de Negocios por Internet

Política:
Los trabajadores de la Institución 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, la solución 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.
Política Dirigida a: Usuarios finales

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 Institución antes de que los sistemas de computación de la Institución 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 adecuada-mente 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.
Política Dirigida a: 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 Institución con ningún contrato, posición o acción, a menos que el trabajador esté especialmente autorizado para constituir contratos a nombre de la Institución, o autorizado de alguna manera para representar legalmente a la Institución.
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 corresponsales 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 corresponsales pueden alegar que confiaron en el correo electrónico y que ejercieron acciones que los perjudicaron y que ahora la Institución 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.
Política Dirigida a: Usuarios finales

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 per-

fil 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 Institución 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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

17. Registros de Telemercadeo
Política:
Los representantes de ventas de la Institución 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 telemercadeo de la Institución, 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.
Política Dirigida a: Gerencia y personal técnico

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 Institución 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.
Política Dirigida a: Personal técnico

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 Institución, 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

IV. Seguridad de Correo Electrónico

1. Revisión de Mensajes de Correo Electrónico de Terceros

Política:
Los trabajadores de la Institución pueden leer los mensajes enviados a través de los sistemas de correos electrónicos de la Institución que permiten el acceso a terceros, sólo si tanto el remitente como el receptor lo han autorizado.
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 Institución 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.
Política Dirigida a: 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.
Política Dirigida a: Todos

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 Institución, 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.

Política Dirigida a: Usuarios finales

4. Información de Contacto del Remitente

Política:

Todo correo electrónico enviado utilizando los sistemas informáticos de la Institución 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 Institución 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.

Política Dirigida a: Usuarios finales

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 Institución 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 Institución siempre indicará el proceso de eliminación asociado a una lista de distribución.

La política implica también que el personal de la Institución 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 Institución. Esta política apoyará a la Institución en sus esfuerzos de cumplir las políticas de privacidad de algunos países.

Política Dirigida a: Personal técnico

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 Institución.

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.
Política Dirigida a: Usuarios finales y personal técnico

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.

Política Dirigida a: Usuarios finales

8. Manejo de Mensajes de Correo Electrónico

Política:

Los administradores de los sistemas de la Institución 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.

Política Dirigida a: Personal técnico

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 Institución.

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.

Política Dirigida a: Usuarios finales

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 elec-

trónico. Tal como ocurre con el respaldo de los datos personales, los usuarios toman en serio esta materia sólo tras la pérdida de material importante.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: 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 respal-

dar 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 Institución, como desde la Institución hacia un cliente.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales

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".
Política Dirigida a: 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.
Política Dirigida a: Usuarios finales y personal técnico

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.

Política Dirigida a: Usuarios finales

18. Restricciones en Contenido de Mensajes

Política:

Los trabajadores no deben enviar o remitir ningún mensaje a través de los sistemas informáticos de la Institución 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 Institución 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 Institución 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 Institución a las actividades del negocio.

Política Dirigida a: Usuarios finales

19. Monitoreo de Contenido de Correo Electrónico

Política:

Los trabajadores deben limitar sus comunicaciones a asuntos de negocios, reconociendo que la Institución 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.

Política Dirigida a: Usuarios finales

20. Mensajes Personales No Solicitados de Correo Electrónico

Política:

Los trabajadores que usen los sistemas informáticos de la Institución 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.
Política Dirigida a: Usuarios finales

21. Correo Electrónico en Volumen
Política:
Los trabajadores no deben utilizar los computadores de la Institución 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 incurriría al resolver dichas quejas. La política aclara que la Institución 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 Institución. La política podría incluir una medida de prohibición de recopilación de respuestas originadas por dichas transmisiones masivas no solicitadas.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales y personal técnico

24. Revisión de Correo Electrónico y Pies de Página

Política:

Todos los servidores de la Institución 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.

Política Dirigida a: Personal técnico

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 Institución distinto al indicado en la cabecera del mensaje y que no constituye necesariamente una posición oficial de la Institución, debe anexarse automáticamente a todos los correos electrónicos salientes que procedan de los computadores de la Institución.

Comentario:

Esta política garantiza que los receptores del correo electrónico originado en la Institución 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 Institución. El lenguaje específico pudiera cambiar de jurisdicción a jurisdicción.

Política Dirigida a: Personal técnico

26. Monitoreo de Mensajes de Correo Electrónico

Política:

La Institución 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 Institución, 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 monitorea-

das 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 acompañarla con una política adicional que prohíba el cifrado en estos casos.
Política Dirigida a: Usuarios finales

27. Archivo y Revisión de Correo Electrónico
Política:
Todo correo electrónico enviado mediante el servidor de correos de la Institución 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales

29. Archivo de Correo Electrónico
Política:
Todos los mensajes de correo electrónico oficiales de la Institución 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.
Política Dirigida a: Todos

30. Usos del Sistema de Correo Electrónico
Política:
Los trabajadores deben usar esencialmente los sistemas de correo electrónico de la Institución 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 Institución 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.
Política Dirigida a: Todos

31. Distribuciones de Correo Electrónico
Política:
La Institución 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.
Política Dirigida a: Usuarios finales

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 autentificar la identidad de los generadores de mensajes de correos electrónicos. Estos incluyen firmas digitales, certificados digitales, cifrado y sistemas de contraseñas dinámicas.
Política Dirigida a: Usuarios finales

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 evitaría 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".
Política Dirigida a: Usuarios finales

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 Institución 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.
Política Dirigida a: Usuarios finales y personal técnico

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 conoci-

miento 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.
Política Dirigida a: Usuarios finales

36. Foros Electrónicos Públicos
Política:
Los trabajadores no deben usar los sistemas informáticos de la Institución 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 Institución 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.
Política Dirigida a: Usuarios finales

V. SISTEMAS PÚBLICAMENTE DISPONIBLES

1. Uso del Nombre de la Organización
Política:
El uso escrito y público del nombre de la Institución 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 Institución 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 Institución. Esta política es un enfoque conservador que refleja gran preocupación por la conservación del buen nombre que disfruta la Institución.
Política Dirigida a: Usuarios finales

2. Secretos Industriales en la Intranet
Política:
Todos los secretos industriales de la Institución 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 Institución 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.
Política Dirigida a: Gerencia

3. Servicios Telefónicos en Internet

Política:
No deben utilizarse los servicios telefónicos de Internet para la transmisión de información secreta no cifrada de la Institución.
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.
Política Dirigida a: Usuarios finales y personal técnico

4. 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.
Política Dirigida a: Usuarios finales

5. 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.
Política Dirigida a: Usuarios finales

6. 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.
Política Dirigida a: Gerencia y personal técnico

7. Sin Responsabilidad en Mensajes

Política:
Un mensaje de renuncia debe colocarse en todos los sitios de la red donde la Institución 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 Institución 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 Institución 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.
Política Dirigida a: Usuarios finales

8. 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 Institución.
Comentario:
Esta política notifica a los usuarios que no deben asumir automáticamente que lo que leen u observan en los sistemas de la Institución es necesariamente política de la Institución. 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".
Política Dirigida a: Usuarios finales

9. Grupos de Discusión en Internet

Política:

Los usuarios no deben usar sus identificadores de usuario de la Institución, para publicar contenido en línea conjuntamente con grupos de discusión polémicos en Internet o en otro foro público.

Comentario:

Esta política evita que la Institución 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 Institución.

Política Dirigida a: Usuarios finales

10. Comunicaciones Salientes en Internet

Política:

Todas las comunicaciones salientes en Internet deben respetar la reputación de la Institución 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.

Política Dirigida a: Usuarios finales

11. 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 Institución, 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 Institución. 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.

Política Dirigida a: Personal técnico

12. Modificación de Información por Internet

Política:

Los usuarios que se conectan con los sistemas de la Institución a través de Internet no deben modificar directamente ninguna información de la Institución.

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 Institución, tales como las bases de datos, los diccionarios de datos, los archivos principales y las páginas en la red. Utilizando mecanismos sólidos de autentificación 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".
Política Dirigida a: Personal técnico

13. 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 Institución.
Comentario:
Esta política blinda a la Institución 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.
Política Dirigida a: Usuarios finales

14. 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 Institución, pueden indicar su afiliación con la Institución.
Comentario:
Esta norma limita el número de representantes oficiales de la Institución 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.
Política Dirigida a: Usuarios finales

15. 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 Institución 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 Institución. 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.
Política Dirigida a: Usuarios finales

16. 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 paternal 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.

Política Dirigida a: Usuarios finales

17. 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 Institución, 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 Institución usando una dirección personal de correo electrónico y otras instalaciones no pertenecientes a la Institución. Algunas organizaciones querrán que el departamento legal quedase a cargo de realizar la mencionada autorización, en lugar del departamento de Relaciones Públicas.

Política Dirigida a: Usuarios finales

18. 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 Institución, 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 nego-

cio de la Institución. El alcance de la política se puede ampliar para incluir salas de charla en Internet.
Política Dirigida a: Usuarios finales

19. Transmisión por Internet de Información Sensible

Política:
No se debe enviar vía Internet la información no cifrada, secreta, patentada o privada de La Institución.
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.
Política Dirigida a: Usuarios finales

20. Avisos Públicos Inadecuados

Política:
El correo electrónico enviado por los trabajadores de la Institución 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 Institución 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 Institución. Esta política intenta hacer que los empleados sean más cuidadosos con lo que publican. La política también otorga a la Institución 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 Institución, incluyendo la afiliación que otorga su dirección del correo electrónico, la Institución 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 Institución. Por ejemplo, si un representante de servicios al cliente de la Institución hizo una declaración personal en un foro público de Internet, dando mala imagen de la Institución, 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 Institución y el operador de sistema implicado. Los derechos legales de la Institución al suprimir el derecho individual a la libre expresión pueden ser un problema aquí y deben discutirse con el grupo de consultoría legal.
Política Dirigida a: Usuarios finales y personal técnico

21. Publicación en Internet de Material

Política:
Los usuarios no deben colocar material de la Institución 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 Institución.
Política Dirigida a: Usuarios finales

22. 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 Institución 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.
Política Dirigida a: Usuarios finales y personal técnico

23. 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 Institución.
Comentario:
Esta política está dirigida a sensibilizar a los trabajadores de la Institución sobre publicaciones 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 Institución 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.
Política Dirigida a: Usuarios finales

24. Transferencia de Archivos Descargados

Política:
Para descargar cualquier archivo de Internet se deben usar computadores que no estén conectados a la red de la Institución 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.
Política Dirigida a: Usuarios finales

25. 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 Institución con información de Internet hasta que ésta sea confirmada por otra fuente.
Política Dirigida a: Usuarios finales

26. Carga de Software

Política:
Los usuarios no deben cargar software que haya sido licenciado por terceros o software que haya sido desarrollado por la Institución, 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 prohibida 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 Institución 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 Institución. 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.
Política Dirigida a: Usuarios finales

27. 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 Institución, debe estar acompañado por la siguiente excepción de responsabilidad: "La admisión por parte de la Institución 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 Institución. 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 Institución, 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 Institución.
Política Dirigida a: Personal técnico

28. 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 Institución 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 confíe 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 confíe únicamente en la información gratuita disponible en Internet. El confiar, en este caso, sería aceptable si la información pudiera ser corroborada de manera independiente.
Política Dirigida a: Personal técnico

29. 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 restauren 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.
Política Dirigida a: Personal técnico

30. Almacenamiento de Información Financiera de Clientes

Política:
La Institución 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.
Política Dirigida a: Personal técnico

31. Información Secreta en la Web

Política:
La información secreta de la Institución 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.
Política Dirigida a: Personal técnico

32. 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 autentificación extendida del usuario, más allá del mero identificador de usuario y contraseña fija que puede requerir el computador de destino. Este nivel adicional de autentificación de usuario puede ayudar aún más a restringir el acceso a la información secreta.
Política Dirigida a: Personal técnico

33. Información de Contacto en Seguridad

Política:
Todas las páginas de apertura de todos los sitios Web de la Institución 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.
Política Dirigida a: Usuarios finales

34. Investigación Pública

Política:

Cada vez que la Institución 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 Institución publica boletines informativos, reportes de investigación o material similar.

Política Dirigida a: Usuarios finales

REQUISITOS PARA EL CONTROL DE ACCESO

I. Política de Control de Acceso

1. Actividades del Hacker

Política:

Los trabajadores no deben utilizar los sistemas informáticos de la Institución 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 Institución 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 autentificación. Esta política puede utilizarse para disciplinar, y tal vez despedir, a un trabajador que realice actividades de "hacking" con los sistemas informáticos de la Institución. Esto es deseable si la organización quiere evitar que esta actividad se revele al público.

Política Dirigida a: Usuarios finales y personal técnico

2. Regulación del Software

Política:

Todo el software instalado en los sistemas multiusuario de la Institución, 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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Gerencia y personal técnico

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 diplomá-

ticas, 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.
Política Dirigida a: Todos

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.
Política Dirigida a: Todos

6. Permisos Predeterminados de Archivo
Política:
Los permisos para el control de acceso de los archivos para todos los sistemas en red de la Institución, 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.
Política Dirigida a: Usuarios finales y personal técnico

7. Mal Funcionamiento del Control de Acceso
Política:
Si un sistema de control de acceso de un 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.
Política Dirigida a: Gerencia y personal técnico

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 Institución. 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 traumatizantes 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

10. Restricciones a la Recopilación de la Información

Política:
Si la información sensible de la Institución 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.
Política Dirigida a: Personal técnico

12. Divulgación de la Información de Terceros

Política:
Los trabajadores de la Institución 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 Institución exigirá un acuerdo de confidencialidad y una autorización previa antes de que cualquier tercero obtenga la información que ha sido confiada a la Institución. 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.
Política Dirigida a: Usuarios finales y personal técnico

13. Solicitudes de Información Organizacional
Política:
Todas las solicitudes de información sobre la Institución y sus actividades de negocios, incluyendo, sin limitantes, cuestionarios, sondeos y entrevistas periodísticas, deben ser referidos 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 Institución 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".
Política Dirigida a: Todos

14. Liberación de Información de la Organización
Política:
Se debe obtener permiso previo de la gerencia principal de la Institución 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.
Política Dirigida a: Todos

15. Solicitudes 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.
Política Dirigida a: Gerencia y personal técnico

16. 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 Institución ofrece sus productos o servicios, también requeriría de autorización. Esta política podría incluir la frase "los trabajadores no deben divulgar más información de la Institución 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.
Política Dirigida a: Todos

17. Autorización de Divulgación de Información
Política:
La divulgación de cualquier archivo almacenado y todo mensaje enviado a través de la red de la Institución 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 ajenas 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.
Política Dirigida a: Usuarios finales y personal técnico

18. Naturaleza y Ubicación de la Información de la Organización

Política:
La información relativa al origen y ubicación de la información sobre la Institución, 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 Institución. 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.
Política Dirigida a: Todos

19. Exploración de Sistemas

Política:
Los empleados no deben explorar los sistemas informáticos o redes de la Institución.
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 Institución, 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.
Política Dirigida a: Todos

20. 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 crítico para la Institución.
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 Institución actuar como sitio beta o probar estos nuevos productos. Sin embargo, sí evita que la Institución 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 Institución 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.
Política Dirigida a: Personal técnico

21. Creación de Herramientas de Seguridad
Política:
Los desarrolladores y diseñadores de los sistemas internos de la Institución 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.
Política Dirigida a: Personal técnico

22. 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.
Política Dirigida a: Personal técnico

23. Uso de Derechos en Sistemas Informáticos
Política:
No deben utilizarse los derechos en sistemas informáticos para cualquier propósito empresarial de la Institución 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.
Política Dirigida a: Personal técnico

24. 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.
Política Dirigida a: Personal técnico

25. Otorgamiento de Acceso a la Información de la Organización
Política:
El acceso a la información de la Institución 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'.
Política Dirigida a: Gerencia y personal técnico

ADMINISTRACIÓN DEL ACCESO DE USUARIO

I. 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.
Política Dirigida a: Personal técnico

2. Identificador de Usuario No Anónimo
Política:
Todos los identificadores de usuario de los computadores y redes de la Institución deben construirse de conformidad con la norma de construcción de identificadores de usuario de la Institución, 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.
Política Dirigida a: Personal técnico

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 Institución.
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 "autentificación positiva del usuario", lo cual permitiría el uso de tarjetas inteligentes, tarjetas de contraseñas dinámicas, biometría y otras tecnologías.
Política Dirigida a: Personal técnico

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 Institución. 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.
Política Dirigida a: Personal técnico

5. Finiquito de los Privilegios de Acceso

Política:
Todos los privilegios informáticos proporcionados por la Institución 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 Institución. A menudo, se ignoran estos asuntos administrativos por atender otros asuntos más inmediatos. En al-

gunos 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 Institución. 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.
Política Dirigida a: Personal técnico

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 Institución, 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.
Política Dirigida a: Usuarios finales

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 evitará 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.
Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

9. Re-Utilización de Identificadores de Usuario

Política:

Todo identificador de usuario dentro del sistema de computadores y de comunicaciones de la Institución 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 Institución.

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.

Política Dirigida a: Personal técnico

10. Norma de Creación para Identificadores de Usuario

Política:

Los identificadores de usuario de un trabajador de la Institución 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.

Política Dirigida a: Personal técnico

11. Múltiples Identificadores de Usuario

Política:

Todos los empleados de la Institución 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.

Política Dirigida a: Usuarios finales

12. Autorización de Solicitud de Acceso al Sistema

Política:

Todas las solicitudes de privilegios adicionales en los sistemas multiusuario o redes de la Institución 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 documen-

tación 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.
Política Dirigida a: Gerencia y personal técnico

13. Privilegios de Identificadores de Usuarios Inactivos

Política:
Después 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.
Política Dirigida a: Gerencia y personal técnico

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 Institución.

Comentario:
Antes de obtener el acceso a cualquier sistema de la Institución, 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Gerencia y personal técnico

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 Institución.
Comentario:
Esta política informa a los usuarios que deben reportar a los administradores de sistemas de la Institución 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.
Política Dirigida a: Usuarios finales

17. Transferencia de Responsabilidad en Custodia
Política:
En el momento en que un trabajador deja su cargo en la Institución, 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.
Política Dirigida a: 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 Institución.
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.
Política Dirigida a: Gerencia

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.
Política Dirigida a: Personal técnico

20. Autentificación para Cuentas Nuevas
Política:
Cada vez que la Institución abra una nueva cuenta con un cliente, debe autentificar 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.
Política Dirigida a: Usuarios finales

II. 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."
Política Dirigida a: Gerencia y personal técnico

2. Restricción de Privilegios — Necesidad de Retener
Política:
El acceso a los sistemas de computación y de comunicaciones de la Institución 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 enfo-

que 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 'necesitar 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 'necesitar 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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

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 reinicializar 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.
Política Dirigida a: Gerencia y personal técnico

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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 normal-mente 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 comuni-

caciones 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

III. 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.
Política Dirigida a: Personal técnico

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 Institución, 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 autentificación 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 tele-trabajadores remotos o clientes que utilicen un servicio de alto riesgo por Internet, tal como el de intercambio de acciones bursátiles.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

6. Reinicialización de la Contraseña Posterior a la Desactivación
Política:
Todos los sistemas de computación de la Institución 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 autentificado.
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 ajenas 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.

Política Dirigida a: Personal técnico

7. Contraseñas en Software

Política:

Las contraseñas nunca deben incorporarse al software desarrollado o modificado por los empleados de la Institución.

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.

Política Dirigida a: Personal técnico

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 restablecimiento 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.

Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

10. Autentificación de Contraseña en Persona
Política:
El usuario debe ser autentificado 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 solicitante 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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Personal técnico

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.

Política Dirigida a: Todos

IV. 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.

Política Dirigida a: Gerencia y personal técnico

CONTROL DE ACCESO A LA RED

I. Política para el Uso de los Servicios de Tejido

1. Descontinuación del Servicio

Política:

La Institución 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 Institución 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 Institución 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 restablecimiento de un ambiente de computación confiable.

Política Dirigida a: Usuarios finales

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 Institución 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.

Política Dirigida a: 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 Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

4. Normas de Telefónicas Comunes

Política:

Los servicios de conexión en la red suministrados por la Institución 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 Institución 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 Institución 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.

Política Dirigida a: Usuarios finales

5. Acceso a la Red Interna

Política:

Sólo los computadores suministrados por la Institución deben tener capacidad para acceder a la red interna de la Institución.

Comentario:

Esta política separa a todos los computadores personales con acceso a la red interna de la Institución, 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 autentificación extendida del usuario se agregue a cada computador personal autorizado y quizás el software de una red privada virtual. Este programa de autentificación 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.

Política Dirigida a: Usuarios finales

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.

Política Dirigida a: Personal técnico

7. Restricción de Acceso a Internet

Política:

El acceso a Internet debe otorgarse solamente a los empleados de la Institución 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.

Política Dirigida a: Usuarios finales y personal técnico

8. Sitios Web No Relacionados con Negocio

Política:

Los sistemas informáticos de la Institución 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.

Política Dirigida a: Usuarios finales

9. Bloqueo de Acceso a Sitios Ajenos al Negocio

Política:

La Institución 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 ad-

ministración 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 listas 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Usuarios finales

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 Institución.
Comentario:
El propósito de esta política es evitar que los empleados utilicen los sistemas de la Institución 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 desearan 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.
Política Dirigida a: Usuarios finales y personal técnico

12. Propiedad Intelectual
Política:
Al acceder a Internet utilizando los sistemas de la Institución, 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 identifican las mismas o revelar información interna de la Institución 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 líbelo, la calumnia, la difamación y otros problemas legales relacionados.
Política Dirigida a: Usuarios finales

II. 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 figura 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.
Política Dirigida a: Personal técnico

III. 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

3. Contraseñas para Computadores Conectados a la Red

Política:
Todos los computadores conectados a la red de la Institución 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 autentificación 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Usuarios finales y personal técnico

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 anterior-mente. 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".

Política Dirigida a: Todos

6. Caracteres de las Contraseñas

Política:

Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabético y otro no alfabético.

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 alfabéticos con los caracteres no alfabéticos.

Se deben tomar en consideración todos los sistemas posibles que utilizan las contraseñas seleccionadas por el usuario y los teclados disponibles, para que se esfuercen por hacer que la política se aplique de manera consistente, tanto como sea posible.

Política Dirigida a: Todos

7. Mayúsculas y Minúsculas en Contraseñas

Política:

Todas las contraseñas seleccionadas por el usuario deben contener por lo menos un carácter alfabético 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 alfabéticos y no alfabéticos 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.
Política Dirigida a: 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 multiplataforma 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 multiplataforma 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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 "IDTP2EAW9" ruegan ser escritas en alguna parte, porque son difíciles de recordar. Por otra parte, las contraseñas generadas por el sistema como "cabellover-decome" 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.

Política Dirigida a: Personal técnico

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 l 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.

Política Dirigida a: Personal técnico

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 computa-dores 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.
Política Dirigida a: Personal técnico

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 divulgan 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.
Política Dirigida a: Personal técnico

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 encimas de ellas mismas, múltiples veces. En ocasiones es posible recuperar las contraseñas de archivos temporales o de ubicaciones casuales en la memoria.
Política Dirigida a: Personal técnico

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 enmascarado 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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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 Institución.

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

19. Información de Control de Acceso en Cookies

Política:

Los sistemas informáticos de la Institución 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 Institución. 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".
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 comprome-

ter 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.
Política Dirigida a: Personal técnico

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 diseminación 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 autentificación 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 de los paquetes tradicionales de control de acceso estilo mainframe.
Política Dirigida a: Personal técnico

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 Institución.
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.
Política Dirigida a: Personal técnico

24. Cambios de Seguridad Después 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 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.

Política Dirigida a: Personal técnico

COMPUTACIÓN MÓVIL

I. 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 Institución, 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 Institución 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.

Política Dirigida a: Usuarios finales

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 Institución.
Comentario:
Esta política prohíbe el uso de computadores pequeños portátiles con información sensible de la Institución 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 Institución en estos pequeños computadores, a pesar de que esto puede degradar adversamente la productividad del trabajador.
Política Dirigida a: Usuarios finales

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 Institución, 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.
Política Dirigida a: Todos

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 Institución 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, tele-trabajadores y asuntos relacionados 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 Institución 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.
Política Dirigida a: Usuarios finales

5. Computadores Portátiles con Información Sensible

Política:

Todos los computadores portátiles, laptops, libretas y otros computadores transportables que contengan información sensible de la Institución, 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. Estas 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.

Política Dirigida a: Todos

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 Institución, 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 recibirlas 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 almacenamientos 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.

Política Dirigida a: 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.
Política Dirigida a: Todos

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 presten 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.
Política Dirigida a: Usuarios finales

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 Institución de robo, daño y abuso.
Comentario:
Esta política notifica a los tele-trabajadores y otros que trabajan con los sistemas informáticos de la Institución 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, ésta se 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.
Política Dirigida a: Usuarios finales y personal técnico

10. Información Almacenada en Computadores Portátiles Propiedad de la Organización

Política:
La información almacenada en computadores portátiles de la Institución es propiedad de ella y la Institución la puede inspeccionar o utilizar de cualquier manera y a cualquier hora y, al igual que el equipo, debe ser devuelta a la Institución al momento en que el empleado cese su relación laboral con la Institución.
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 Institución puede examinar su contenido en cualquier momento. Esta política extiende los límites entre la propiedad organizacional y la pro-

piedad 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.
Política Dirigida a: Usuarios finales

11. Posesión de los Computadores Portátiles
Política:
Los empleados deben mantener los computadores portátiles de la Institución 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.
Política Dirigida a: Usuarios finales

12. Alternativas para Computadores Móviles
Política:
Cuando estén fuera de las oficinas de la Institución, 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 Institución 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 Institución contenida en un computador móvil.
Política Dirigida a: Usuarios finales

14. Equipo de Teletrabajo
Política:
Los empleados de la Institución que trabajen en sitios alternativos deben utilizar computadores y equipos de redes proporcionados por la Institución, a menos que el Centro de Atención al Usuario autorice el uso de otro equipo compatible con los sistemas y controles informáticos de la Institución.
Comentario:
Esta política garantiza que los tele-trabajadores no utilizarán sistemas informáticos que puedan causar un mal funcionamiento o daño a los sistemas o a la información de la Institución, o no proporcionen protección suficiente a la información de la Institución. 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 tele-trabajadores. Esta lista puede incluir un modem, una línea telefónica de alta velocidad, buscapersonas, 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 Institución no es responsable por pérdidas, daños o uso y desgaste de un equi-

po propiedad del empleado utilizado para negocios de la Institución. 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 Institución. Estas políticas se deben complementar con palabras que definan lo términos como "sitio alternativo de trabajo" y "teletrabajo".
Política Dirigida a: Usuarios finales y personal técnico

15. Ambientes de Teletrabajo

Política:
Para retener el privilegio de trabajar externamente, todos los tele-trabajadores deben estructurar su ambiente de trabajo remoto para que esté de acuerdo con las políticas y normas de la Institución.
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 Institución. 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.
Política Dirigida a: Usuarios finales

16. 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 Institución.
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 Institución. 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".
Política Dirigida a: Todos

17. 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 si-

tios 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.
Política Dirigida a: Usuarios finales

18. Inspección de Ambientes de Teletrabajo
Política:
La Institución 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 Institución 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 Institución 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 Institución 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.
Política Dirigida a: Usuarios finales

19. Gabinetes Metálicos con Cerradura
Política:
Todos los trabajadores que deban mantener información confidencial de la Institución 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 Institución 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 Institución. 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.
Política Dirigida a: Gerencia

CONTROLES CRIPTOGRÁFICOS

I. 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 en 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.

Política Dirigida a: Usuarios finales y personal técnico

II. Cifrado

1. Autorización del Proceso de Cifrado — Sistemas

Política:

Los procesos de cifrado no deben ser utilizados para la información de la Institución, 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 Institución 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.

Política Dirigida a: Usuarios finales

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 Institución 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.
Política Dirigida a: Usuarios finales

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 está incrustado 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Personal técnico

5. Algoritmos de Cifrado Evaluados Públicamente
Política:
Todo algoritmo de cifrado de propósito general utilizado para proteger la información de producción de la Institución 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.
Política Dirigida a: Personal técnico

6. Inicialización del Sistema de Cifrado
Política:
Siempre que se inicialice, instale, active o reinicialice un sistema de cifrado que se utilizará en los sistemas informáticos de producción de la Institución, 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.
Política Dirigida a: Personal técnico

7. Eliminación de Datos Fuente Después 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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

10. 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 Institución, deben cifrarse utilizando software normal de la Institución.
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.
Política Dirigida a: Usuarios finales y personal técnico

III. 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 Institución. Esta política asume que los usuarios pueden distinguir entre 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.
Política Dirigida a: Usuarios finales

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 Institución y al que puedan conectarse clientes, prospectos y demás personas.
Comentario:
Esta política evita que terceros establezcan sistemas en Internet que se disfracen como sistemas de la Institución. 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 Institución. 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.
Política Dirigida a: Usuarios finales

IV. 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 Institución 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 autentificación 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.
Política Dirigida a: Personal técnico

V. 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.
Política Dirigida a: Personal técnico

2. Sistemas de Gestión de Claves de Cifrado

Política:
El sistema de cifrado de la Institución, 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.
Política Dirigida a: Personal técnico

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 Institución 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.
Política Dirigida a: Gerencia y personal técnico

4. Vigencia de los Certificados Digitales

Política:

El período de validez para certificados digitales emitidos por la Institución 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 Institución. 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 período 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 corresponsales 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.

Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 manejos 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.
Política Dirigida a: Personal técnico

7. Gestión Automática de Claves de Cifrado
Política:
Si están disponibles comercialmente, la Institución debe emplear procesos automatizados de gestión de claves.
Comentario:
Esta política ahorra dinero y tiempo a la Institución, 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 interoperabilidad con otros sistemas de gestión de claves.
Política Dirigida a: Personal técnico

8. Ciclo de Vida de Claves de Cifrado
Política:
Las claves utilizadas para el cifrado de datos de la Institución 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 la 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.
Política Dirigida a: Personal técnico

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 valido por una sola vez. Los cifrados validos 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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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, ini-

cialización 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.
Política Dirigida a: Personal técnico

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".
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 les 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. Está 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.
Política Dirigida a: Usuarios finales y personal técnico

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.
Política Dirigida a: Usuarios finales

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 pertenecen. Si los usuarios simplemente almacenan la versión legible de sus claves privadas en el disco duro de un computador perso-

nal, 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.
Política Dirigida a: Usuarios finales

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 adecuada-mente 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.
Política Dirigida a: Personal técnico

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 divulgan, 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.
Política Dirigida a: Personal técnico

21. Seguridad de Clave Privada para Certificados Digitales
Política:
La clave privada asociada a cada trabajador en la Institución 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.
Política Dirigida a: Usuarios finales

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.

Política Dirigida a: Personal técnico

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.

Política Dirigida a: Personal técnico

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 corresponsales 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 corresponsales 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 corresponsales de futuros cambios a una clave pública pueden firmarse con una clave privada que aún no haya vencido. Esto les asegura a los corresponsales que han recibido un mensaje del usuario legítimo y no de un impostor.

Política Dirigida a: Todos

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.
Política Dirigida a: Personal técnico

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 almacenamientos no cifrado de estos materiales de cifrado.
Política Dirigida a: Personal técnico

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 Institución, 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.
Política Dirigida a: Personal técnico

28. Claves de Cifrado de Respaldo

Política:
Si el trabajador de la Institución 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.
Política Dirigida a: Usuarios finales

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 responsabilidad 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.
Política Dirigida a: Gerencia y personal técnico

SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

I. Revisión Técnica de los Cambios en Sistemas Operativos

1. Configuración del Sistema Operativo

Política:

El personal técnico de la Institución 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.

Política Dirigida a: Personal técnico

2. Parches de Software, Arreglos y Actualizaciones

Política:

Todos los sistemas de producción en la red de la Institución 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.

Política Dirigida a: Personal técnico

II. 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 suplidas 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.
Política Dirigida a: Personal técnico

2. Acceso de Proveedor Tercero a Software Empacado

Política:
Los paquetes de software de terceros que la Institución 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 Institución.
Comentario:
Esta política evita que la Institución 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 suplidas por un proveedor de servicio de aplicaciones.
Política Dirigida a: Personal técnico

II. Desarrollo de Software con Terceros

1. Desarrollo de Software por Terceros

Política:
Los terceros que desarrollen software para la Institución 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 Institución, 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 Institución con respecto a la funcionabilidad 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 Institución, la obligatoriedad de un convenio firmado suministra a la Empresa el soporte legal necesario para resolver cualquier disputa.
Política Dirigida a: Gerencia y personal técnico

ASPECTOS DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

I. 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 Institución.

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.
Política Dirigida a: Personal técnico

II. 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".
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

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 Institución 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.
Política Dirigida a: Personal técnico

III. 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".
Política Dirigida a: Personal técnico

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 con-

tingencia 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.
Política Dirigida a: Gerencia y personal técnico

IV. 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.
Política Dirigida a: Gerencia y personal técnico

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 Institución, 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 Institución. 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 Institución.
Política Dirigida a: Usuarios finales

V. 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 Institución 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.

Política Dirigida a: Personal técnico

2. Rotación del Personal Fuera de Sede

Política:

Los empleados que participen en operaciones de recuperación fuera de sede con sistemas informáticos de la Institución, 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 crucial-mente 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.

Política Dirigida a: Personal técnico

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 desas-

tre 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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Gerencia y personal técnico

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.
Política Dirigida a: Personal técnico

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.
Política Dirigida a: Personal técnico

Bibliografía

Código de Practica para la administracion de la Seguridad de la Información. IDAM, Instituto Argentino de Normalizacion (2002) - ISO/IEC 17799:2005

Guide to Networking Essentials, Greg Tomsho, Ed Tittel, and David Johnson - 3era Edición (2002) – Course Technology

Foro Permanente de Responsables Informáticos de la Administración Pública Nacional, Actas e Informes del Foro de Responsables Informáticos - (2002-2003-2004-2005) http://rrii.sgp.gov.ar/

Prácticas de Seguridad en Sistemas Conectados a Internet, Juan Manuel da Costa Palacios (2003) – LibrosEnRed

Fundamentos de Seguridad de Redes, Eric Maiwald (2004) – McGraw Hill, Segunda Edición

Fundamentos de Seguridad de Redes - Especialista En Firewall Cisco, Academia de Redes Cisco (2006) – Pearson Education