Guía de Seguridad Informática

Guía de Seguridad Informática

CONTENIDO

INTRODUCCION

Segregación de Responsabilidades
Incidentes de Seguridad y Procedimiento Disciplinario
Gestión Externa de Servicios (Outsourcing)
La Seguridad informática como Imperativo Legal

POLITICAS Y ORGANIZACION DE SEGURIDAD

1.1 Análisis de Riesgos
    1.1.1 Sus Componentes
    1.1.2 La Realización del Análisis
1.2 Políticas de Seguridad
    1.2.1 Normas de Seguridad Informática
    1.2.2 Procedimientos de Seguridad Informática
    1.2.3 La Calidad en la Seguridad
1.3 Organización en la Empresa
    1.3.1 Consideraciones Organizativas
    1.3.2 Factores Críticos de Exito
1.4 Infraestructura de Seguridad Informática
    1.4.1 En la Dirección de la Empresa
    1.4.2 En la Función de Sistemas de Información
    1.4.3 En las restantes Funciones de Empresa
    1.4.4 Soporte de Especialistas en Seguridad Informática
1.5 Actores y sus Responsabilidades
    1.5.1 Propietario
    1.5.2 Depositario
    1.5.3 Usuario

CLASIFICACION DE ACTIVOS DE INFORMACION

2.1 Niveles de Clasificación
2.2 Marcado de Clasificación
2.3 Protección de la Información Clasificada
    2.3.1 Protección de la Información Impresa
    2.3.2 Divulgación de Información Clasificada
    2.3.3 Transporte de Información Clasificada
    2.3.4 Destrucción de Información Clasificada

PROTECCION FISICA

3.1 Características de Construcción
3.2 Distribución de las Areas
    3.2.1 Areas de Acceso Limitado (AAL)
    3.2.2 Areas de Acceso Restringido (AAR)
    3.2.3 Valoración de las Areas
3.3 Medios de Protección
    3.3.1 Sistemas de Control de Accesos
    3.3.2 Sistemas de Detección
    3.3.3 Sistemas de Extinción de Incendios
3.4 Suministros Auxiliares
    3.4.1 Energía Eléctrica

3.4.2 Acondicionamineto de Aire
3.5 Emergencia y Evaluación
3.6 Medios de Almacenamiento
3.6.1 Protección Física
3.6.2 Protección durante Traslados
3.6.3 Inventario y Reconciliación
3.7 Impresoras

PROTECCION LOGICA

4.1 Indentificación de Usuarios
4.1.1 Identificador de Usuario
4.1.2 Identificador de Usuario Compartido
4.1.3 Autorización de Usuario
4.1.4 Eliminación de Usuario
Revisión de Vigencia
Usuarios Inactivos
4.1.5 Revalidación Anual de Usuarios
4.2 Autentificación de Usuarios
4.2.1 Contraseñas (Passwords)
Restauración de Contraseñas
4.2.2 Contraseñas de una Sola Vez
4.3 Activos de Información del Sistema
4.3.1 Control de Acceso Público
4.3.2 Activos Sensibles del Sistema
4.4 Activos de Información de Usuario
4.4.1 Control de Acceso Público
Revisión Periodica
4.4.2 Activos Sensibles de Usuario
4.4.3 Protección en Desarrollo
Separación de los Sistemas de Desarrollo y Producción
Uso del Estado Supervisor (SVC)
4.4.4 Protección de Terminales
Revisión Periódica
4.4.5 Cifrado o Criptografiado
Claves de Cifrado
Protección de Claves de Cifrado
Responsabilidades
4.4.6 Virus informático y otros Códigos Dañinos
Protección en LAN y PC
Protección en Sistemas Corporativos
4.5 Gestión de Autoridad de Sistema
4.6 Gestión de Autoridad de Administración de Seguridad
4.7 Registro de Intentos de Acceso
4.7.1 Registros de Acceso al Sistema
4.7.2 Registro de Acceso a Activos
4.7.3 Registro de Actividades
4.8 Informes de Violación de Acceso
4.8.1 Acceso Inválidos al Sistema
Ataques Sistemáticos
4.8.2 Accesos Inválidos a Activos

CONEXIONES EXTERNAS

5.1 Responsabilidades
5.1.1 Del Propietario de la Conexión
5.1.2 Del Propietario del 'Gateway'
5.1.3 Del Usuario
5.2 Certificación de la Conexión
5.2.1 Revisión Inicial
5.2.2 Revisión Anual de Recertificación

5.2.3 Suspensión de la Conexión
5.2.4 El Equipo Revisor
5.3 Autorización de Acceso
Conexión DESDE el Exterior
Conexión HACIA el Exterior
Interconexión de Redes y Sistemas
5.4 Conexión a Redes Inseguras
5.4.1 Riesgos en Redes Inseguras
5.4.2 Medidad de Protección
5.4.3 Sistemas Firewall (Cortafuegos)
Sistema de Filtro de Paquetes
Sistema de Servicio
5.5 Transferencia de Activos
5.5.1 Correo Electrónico (Electronic Mail)
5.5.2 EDI (Electronic Data Interchange)
Seguridad y Protección de Activos EDI
5.6 Registros Auditables
5.7 Acuerdos con Terceros
5.8 Glosario de Términos

RECUPERACION DE DESASTRES

6.1 Identificaciones Previas
6.1.1 Aplicaciones y Activos Criticos
6.1.2 Sistemas Esenciales
6.1.3 Centro Alternativo
6.1.4 Revalidación Periódica
6.2 Copias de Respaldo (Backups)
6.2.1 Almacenamiento en el Centro Alternativo
6.2.2 Almacenamiento en el propio Centro
6.2.3 Respaldo Funcional Complementario
6.3 Pruebas de Continuidad
6.3.1 En el Centro Alternativo
6.3.2 En el Propio Centro
6.3.3 Recuperación del Centro Siniestrado
6.4 Situación de Desastre
6.4.1 Continuidad de Operaciones

PROGRAMAS PREPARATORIOS Y DE CONTROL

7.1 Organización de Seguridad
7.2 Formación de Empleados
7.3a Pruebas de Integridad de Sistemas
7.3b Inventario y Clasificación de Activos
7.4 Diagnósticos de Seguridad
7.5 Recuperación de Desastres
7.6 Otras Actividades de Seguridad

ANEXO1. EXTRACTO DE NORMATIVA LEGAL

LORTAD
Artículo 9. Seguridad de los Datos
Artículo 27(.2). Prestación de servicios de tratamiento automatizado
Artículo 43(.3h). Tipos de Infracciones
Ley de Facturación Telemática
Artículo 4(.2f)
Artículo 5(.2d)
Artículo 6(.1)
Artículo 7(.b)

Ley de Ordenación de las Telecomunicaciones
- Artículo 5(.4)
- Artículo 24

Real Decreto 1382/85
- Dispongo
- Artículo 1. Ambito de Aplicación
- Artículo 2. Fundamento
- Artículo 3. Fuentes y Criterios reguladores

Nuevo Código Penal
- Artículo 197
- Artículo 256
- Artículo 264(.2)
- Artículo 278
- Artículo 400

GUIA DE SEGURIDAD INFORMATICA

PREFACIO

Esta publicación ha sido coordinada por **SEDISI (Asociación Española de Empresas de Tecnologías de la Información)**, y está basada en las Normas y Procedimientos de Seguridad Informática utilizadas en importantes empresas nacionales y multinacionales, dedicadas a la fabricación de Recursos Informáticos, al desarrollo de Productos Informáticos y/o al suministro de Servicios Informáticos.

RECONOCIMIENTO SEDISI

Agradece la colaboración, para la elaboración de este documento, de las compañías y organizaciones siguientes:

Alcatel Sistemas de Información o Anyware Seguridad Informática

IBM ISS

Indra

SEMA Group

Tandem Computers

Sin cuya inestimable contribución no hubiera sido posible su publicación.

ACLARACIÓN

No debe confundirse la Seguridad Informática con otras áreas de la Seguridad en la empresa como son las relativas a la seguridad de las personas o de las cosas. La Seguridad Informática también se ocupa de aspectos físicos pero sólo en lo relativo a zonas en las que haya Recursos Informáticos y de los accesos a estas zonas, y de aspectos relativos a las personas pero sólo en lo relacionado con la protección de los Activos de Información y sus accesos a ellos. A lo largo de esta Guía se hablará de Seguridad Informática o de Seguridad indistintamente, pero en ambos casos se estará haciendo referencia a la primera.

PROPÓSITO

Esta Guía está pensada para: o ser usada como referencia por los directivos de la empresa y los responsables de Seguridad Informática. o servir como referencia de términos comunes para el intercambio de información entre empresas y para subcontratistas o proveedores de Servicios y/o Productos Informáticos. o invitar a las empresas a considerar la adopción de este documento como base y ayuda para la definición de sus Políticas de Seguridad Informática y la creación de las Normas y Procedimientos subsiguientes.

APLICACIÓN

No todos los controles que se citan en esta Guía serán aplicables a todas las organizaciones. Los que aquí se exponen responden a los utilizados por organizaciones experimentadas y deben ser tomados como punto de partida para desarrollar los específicos de cada empresa. Cada apartado de la Guía se ha desarrollado en base a la importancia de los Sistemas de Información y no a su tamaño, por lo que podrán aplicarse a cualquier tipo de Sistemas.

INTRODUCCION

Objetivos Generales:

Sentar las bases para el establecimiento de una forma común de gestionar la Seguridad Informática en las empresas que quieran implantar medidas efectivas para la protección de sus Sistemas de Información.

definiendo políticas y normas de Seguridad;

desarrollando procedimientos y métodos de Seguridad;

divulgando la protección requerida e involucrando en ella a todos los empleados;

valorando los riesgos de la instalación;

creando planes de implantación de las medidas de protección;

instaurando controles e indicadores para el mantenimiento del adecuado nivel de protección;

revisando periódicamente el cumplimiento de estos objetivos.

Un Sistema de Información es un elemento de gestión cada vez más importante, en la medida que la empresa incrementa su dependencia de ellos. Está compuesto por los Recursos Informáticos, considerados como el continente o soporte informático, y los Activos de Información, considerados como el contenido.

A lo largo de esta Guía se hará referencia a:

Sistemas de Información o, de forma abreviada, Sistemas.

Recursos Informáticos o, abreviado, Recursos y

Activos de Información o, en abreviatura, Activos o simplemente Información.

Todas estas formas de expresión deben entenderse como sinónimos de las primeras.

La Seguridad Informática permite compartir los Sistemas de Información de la empresa entre sus empleados, e incluso con terceros, pero garantizando su protección. La Seguridad tiene tres aspectos básicos que son esenciales para el crecimiento del negocio, el cumplimiento de la legalidad vigente y la imagen de la propia empresa:

1. CONFIDENCIALIDAD: Protege los Activos de Información contra accesos o divulgación no autorizados.

2. INTEGRIDAD: Garantiza la exactitud de los Activos de Información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

3. DISPONIBILIDAD: Asegura que los Recursos Informáticos y los Activos de Información pueden ser utilizados en la forma y tiempo requeridos. Bajo el punto de vista de Seguridad, la disponibilidad se refiere a su posible recuperación en caso de desastre (Recuperabilidad), y no al concepto de Nivel de Servicio empleado en otras áreas.

Estos aspectos llevan implícitos los conceptos de Propiedad, Depósito y Uso, de los Recursos Informáticos y Activos de Información, que posteriormente se desarrollarán.

Segregación de Responsabilidades

Ciertas tareas (o áreas de responsabilidad) no pueden ser realizadas por la misma persona, a fin de reducir oportunidades de alteración no autorizada o mal uso de los Sistemas de Información. Para ello es fundamental la segregación de responsabilidades, que minimiza el riesgo de mal uso accidental o deliberado del Sistema de Información. En organizaciones pequeñas, este control puede ser difícil de lograr, pero tiene que ser aplicado en la medida que sea factible.

Este control es particularmente importante para Sistemas que soporten aplicaciones más proclives al fraude. Incidentes de Seguridad y Procedimiento Disciplinario Un Incidente de Seguridad es cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas o financieras para la empresa.

Algunos ejemplos a tener en cuenta, son los siguientes:

un acto intencionado, o aparentemente intencionado, cuyo objetivo sea la utilización, manipulación,destrucción o revelación no autorizadas de cualquier Activo de Información;

la transgresión, accidental o deliberada, de los controles de protección de los Recursos Informáticos o Activos de Información que pueda ocasionar perjuicios a la empresa;

divulgar alguna deficiencia en los controles de seguridad existentes;

cualquier acto que, sin ocasionar daño o pérdida material, sea una clara infracción de las políticas, normas o procedimientos de Seguridad definidos en la empresa.

Tiene que formalizarse un Procedimiento Disciplinario para tratar los incidentes de Seguridad, que debe ser elaborado conjuntamente por los departamentos de Recursos Humanos y Sistemas de Información, aprobado por el Comité de Dirección y posteriormente divulgado a todos los empleados, para su conocimiento.

Importante.La inexistencia de medidas disciplinarias compromete gravemente la aplicación de las normas de Seguridad.

Gestión Externa de Servicios (Outsourcing) .El uso de una empresa externa para la gestión de los servicios informáticos (de proceso o de red), implica la cesión de ciertos aspectos de la administración de Seguridad del sistema, pero no del control global de la Seguridad, que debe permanecer en la empresa.

Esta cesión parcial no debe suponer ningún riesgo adicional, para la Seguridad Informática de la empresa, y debe incorporarse al contrato definiendo las responsabilidades de las partes, entre las que cabe destacar las siguientes:

el mantenimiento de los planes de recuperación de la actividad o el negocio;

los procedimientos para el manejo de los incidentes de Seguridad;

las revisiones periódicas del nivel de cumplimiento.

La Seguridad Informática como Imperativo Legal. La legislación española contiene diversas referencias a la seguridad en entornos informáticos. En algunos casos, la referencia es simplemente a modo de recomendación. En otros, tiene un contenido obligatorio.

A continuación se relacionan las principales leyes en las que se exige un sistema que garantice la seguridad de un entorno informático:

LORTAD (artículos 9, 27.2, 43.3.h, etc.);

Nuevo Código Penal;

Ley de Facturación Telemática (artículos 4.2.f, 5.2.d, 6.1 y 7.b);

Ley de Ordenación de las Telecomunicaciones (artículos 5.4 y 24), etc.

1. Políticas y Organización de Seguridad

Objetivos :

Establecer las Políticas y Normas de Seguridad Informática y definir los responsables de su desarrollo, implantación y gestión.

Analizar los riesgos existentes sobre los Sistemas de Información y establecer las acciones necesarias para su reducción o eliminación.

Establecer la función de Seguridad Informática para gestionar la protección de los Recursos Informáticos y los Activos de Información de la empresa.

1.1 ANÁLISIS DE RIESGOS

La Seguridad Informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información. Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.

Para ello, deben utilizarse métodos formales de análisis de riesgos que lo garanticen.

1.1.1 Sus Componentes

En un proceso de Análisis de riesgos se pueden establecer los siguientes componentes:

Sistema de Información. Son los Recursos Informáticos y Activos de Información de que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

Amenaza. Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la empresa pérdidas materiales o financieras.

Vulnerabilidad. Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas para causarles daño y producir pérdidas a la empresa.

Impacto. Es la medición (y valoración) del daño que podría producir a la empresa la materialización de una amenaza sobre los Sistemas de Información. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, que siempre será subjetiva, de los daños intangibles.

Riesgo. Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la empresa.

Defensa. Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste.

1.1.2 La Realización de Análisis

En el proceso de Análisis de riesgos se pueden diferenciar:

1. La Evaluación de Riesgos, orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por

amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la empresa.

2. La Gestión de Riesgos, que implica la identificación, selección, aprobación y manejo de las defensas (contra medidas) para eliminar, o reducir a niveles aceptables, los riesgos evaluados, con actuaciones tendentes a:

reducir la posibilidad de que una amenaza ocurra;

limitar el impacto de una amenaza, si ésta se manifiesta;

reducir o eliminar una vulnerabilidad existente;

permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros).

Un primer análisis de riesgos será mucho más costoso que los sucesivos.

Puede requerir mucho tiempo y la participación de personal cualificado y especializado. El tiempo empleado estará en proporción a los objetivos fijados y a su ámbito de cobertura.

Para resaltar la necesidad de sucesivos análisis de riesgos se deben tener en cuenta las siguientes consideraciones:

Los elementos que componen los Sistemas de Información de una empresa están sometidos a constantes variaciones: nuevo personal informático, nuevas instalaciones, nuevos productos, nuevas aplicaciones, etc.

Pueden aparecer nuevas amenazas o variar la probabilidad de que ocurra alguna de las existentes, afectando al posible impacto.

Pueden aparecer nuevas vulnerabilidades o variar (o desaparecer) alguna de las existentes, creando o eliminando posibles amenazas.

En consecuencia, es necesario actualizar periódicamente el análisis de riesgos tomando como base de partida el último realizado y las defensas implantadas hasta la fecha, por lo que los factores tiempo y medios necesarios para su realización serán menores.

El análisis de riesgos, además de centrarse en los Sistemas de Información existentes, es recomendable aplicarlo en el desarrollo de nuevos Sistemas, asegurándolos desde su creación.

1.2 POLÍTICAS DE SEGURIDAD

La Dirección de la empresa es responsable de definir y publicar las Políticas de Seguridad como una firme declaración de intenciones, así como de divulgarlas en todo el ámbito de la empresa.

El conjunto de las Políticas de Seguridad debe establecer los criterios de protección en el ámbito de la empresa y servir de guía para la creación de las Normas de Seguridad.

1.2.1 Normas de Seguridad Informática

Basándose en las Políticas de Seguridad, la Dirección de la empresa publicará las Normas de Seguridad, en las que se definirá qué hay que proteger y el objeto concreto de esa protección. Una Norma debe ser breve, concisa y redactada en términos claros y comprensibles por todos los empleados, y debe contener como información de control, al menos:

fecha de publicación;

fecha de efectividad o entrada en vigor;

fecha prevista de revisión o renovación;

si es aplicable a toda la empresa o a un ámbito más reducido;

si sustituye a una norma precedente o es nueva.

Las Normas son de obligado cumplimiento, por lo que deben ser divulgadas, de acuerdo con su ámbito de aplicación, a todos los empleados involucrados, incluido el personal directivo.

La responsabilidad del cumplimiento de las Normas es de todos los empleados, pero especialmente del personal directivo que acumula a su responsabilidad como empleado, la de todos los empleados a los que dirige, coordina o supervisa. (Los artículos 133 y 134 de la Ley de Sociedades Anónimas y el Real Decreto 1382/85, establecen supuestos en los que la alta dirección de la empresa puede llegar a ser responsable a nivel individual, por acciones u omisiones que perjudiquen a la sociedad, a sus accionistas o a sus acreedores.)

El conjunto de todas las Normas de Seguridad debe cubrir la protección de todos los entornos de los Sistemas de Información de la empresa.

1.2.2 Procedimientos de Seguridad Informática

Basándose en las Normas de Seguridad, y dependiendo del ámbito de aplicación, el departamento responsable creará los Procedimientos de Seguridad, en los que se describirá cómo proteger lo definido en las Normas y las personas o grupos responsables de la implantación, mantenimiento y el seguimiento de su nivel de cumplimiento. Un Procedimiento debe cubrir todo los aspectos descritos en la Norma que le soporta, siguiendo de forma detallada y concreta todos los pasos en los que se estructura.

En un Procedimiento se deben declarar todas las actividades que lo componen y definir todos los controles necesarios (y sus indicadores de seguimiento) para cumplir con los requerimientos definidos en la Norma correspondiente. Adicionalmente, debe contener como información de control, al menos: o fecha de publicación; o fecha de efectividad o entrada en vigor; o fecha prevista de revisión o renovación; o responsable de su revisión y publicación; o relación de actividades; o responsables de cada actividad; o relación de controles por actividad; o valores críticos de los indicadores; o si sustituye a un procedimiento anterior o es nuevo.

1.2.3 La Calidad en la Seguridad

Teniendo en cuenta criterios de Calidad, los procedimientos, y las actividades que lo componen, pueden estructurarse de tal manera que se podría definir un Proceso por cada procedimiento.

En una segunda fase, las actividades que componen cada procedimiento (ahora proceso) deberían analizarse para evaluar si son, o no, automatizables. Posteriormente, se procedería a la automatización de las actividades que se hubieran declarado viables y a un segundo análisis y evaluación de las restantes actividades. De esta forma, paso a paso, se podría llegar a unos niveles de automatización que minimizarían la intervención humana, excepto en alguna toma de decisiones, obteniendo como valor añadido la fiabilidad de estos procesos.

Siguiendo con los criterios de Calidad, los procesos deben ser revisados periódicamente, como Mejora Continua, para la eliminación de defectos y la reducción del ciclo. Finalmente, resumir los objetivos de la aplicación de la Calidad en el área de Seguridad:

incrementar la fiabilidad de los controles y sus indicadores, proporcionando alertas automáticas;

disminuir la intervención humana, con una reducción adicional del coste de personal;

reducir el ciclo de los procesos, permitiendo obtener información más actualizada.

1.3 ORGANIZACIÓN EN LA EMPRESA

La Dirección debe ser consciente de las facilidades que existen para acceder a los Recursos Informáticos y Activos de Información e incluso manipularlos, sin motivos basados en el negocio de la empresa, es decir: sin autorización.

1.3.1 Consideraciones

Organizativas Generalmente, la empresa tiene una organización jerárquica en forma piramidal, cuyo vértice está ocupado por la más alta dirección. Entre el vértice y la base suele haber varios niveles intermedios, que variarán en número dependiendo del tamaño de la empresa.

Un departamento, o grupo de departamentos homogéneos, forma lo que llamaremos una Función (ej.: Personal, Finanzas, Administración, etc.) con un director funcional al frente de cada una.

Entre ellas, destacamos la función de Sistemas de Información, entendiendo bajo este nombre a los departamentos encargados de gestionar los Recursos Informáticos y los Activos de Información de las restantes funciones de la empresa.

En la medida que cada Función y el negocio de la empresa dependa de la información, la necesidad de protección será más perentoria y cada vez tendrá que ser más sofisticada. Para gestionar esta protección, es necesario contar con una Infraestructura de Seguridad Informática con la formación, dedicación y herramientas especializadas adecuadas.

1.3.2 Factores Críticos de Éxito

Para tener unas mínimas garantías de éxito, en la implantación de la Seguridad Informática en la empresa, la experiencia ha demostrado que son críticos, al menos, los factores siguientes:

El compromiso y apoyo visible de la alta Dirección.

Los objetivos y actividades de Seguridad que deben estar basados en las necesidades de la empresa y liderados por la organización responsable de la Seguridad Informática.

El análisis de riesgos potenciales (y su valoración) para evitarlos o minimizarlos.

La implantación de controles para la detección de riesgos potenciales y su divulgación en todo el ámbito de la empresa.

La rapidez en la actuación para proteger los Sistemas de Información, con lo que los riesgos serán menores y se reducirá sustancialmente el coste de la Seguridad Informática, a medio y largo plazo.

1.4 INFRAESTRUCTURA DE SEGURIDAD INFORMÁTICA

No existe un único modelo predefinido, variará en función del tamaño de la empresa, del volumen y tipo de Recursos y Activos a proteger y del nivel tecnológico alcanzado. Normalmente, podrán utilizarse los recursos humanos existentes en la empresa.

Hay que tener en cuenta que, dependiendo del tamaño de la empresa, algunos puestos no siempre serán cubiertos y que varios puestos pueden ser desempeñados por la misma persona, siempre que no entren en conflicto con el principio de segregación de responsabilidades. Una organización tipo podría ser de la forma siguiente:

1.4.1 En la Dirección de la Empresa

Comité de Dirección:Formado por los Directores Funcionales y con la responsabilidad del nombramiento de Propietarios, a propuesta del Director Funcional correspondiente.

Ejecutivo de Seguridad Informática. Habitualmente, el Director de la Función de Sistemas de Información, dependiendo del más alto nivel de Dirección de la Empresa.

Comité de Seguridad Informática. Formado por todos los Coordinadores Funcionales y el Director responsable de Seguridad Informática.

1.4.2 En la Función de Sistemas de Información

El Director de Sistemas de Información, del que depende o el Director de Seguridad Informática; del que, a su vez, dependerán

el Coordinador de Seguridad Informática;

el Administrador Central de Seguridad Informática;

el Administrador de Usuarios y Accesos;

los Administradores Locales de Seguridad Informática.

1.4.3 En las Restantes Funciones de la Empresa o Coordinador

Funcional de Seguridad Informática. Dependiendo directamente del Director de la Función correspondiente.

Especialistas Informáticos, que asesorarán a sus Coordinadores.

1.4.4 Soporte de Especialistas en Seguridad Informática

Cada empresa, independientemente de su tamaño, debe poder contar con la utilización de especialistas en Seguridad de Informática. Siempre que sea posible, este soporte debe ser dado por un asesor interno, aunque es habitual la contratación de asesores ajenos a la empresa.

Los especialistas deben poder asesorar sobre todos, y cada uno de, los aspectos de la Seguridad Informática. Tienen que valorar el nivel de implantación de las Políticas y Normas de Seguridad Informática y el nivel de cumplimiento de los procedimientos establecidos. Tienen que poder analizar los riesgos: definiendo las posibles amenazas, detectando las vulnerabilidades existentes y determinando las medidas a tomar para su eliminación o reducción. Los especialistas de Seguridad Informática deben ser consultados lo mas rápidamente posible cuando se sospechen incidentes o debilidades de Seguridad, para que establezcan planes de actuación y métodos de aislamiento e investigación del problema.

El mantenimiento y mejora de los niveles de Seguridad adquiridos, es una de las más importantes actividades a realizar en la empresa. Para ello es preciso establecer diagnósticos periódicos, a realizar por especialistas internos, consultores externos independientes o empresas especializadas en consultorías o asesorías de Seguridad.

1.5 ACTORES Y SUS RESPONSABILIDADES

Recomendación:

Para conseguir una Seguridad efectiva y completa de los Recursos Informáticos y Activos de Información, es imprescindible delimitar las funciones y definir las responsabilidades de quienes lo utilizan.

Los Recursos Informáticos y Activos de Información son propiedad de la empresa, pero es necesario delegar en los actores que desempeñan las distintas funciones en la protección y asignar a cada uno de ellos sus responsabilidades.

Este proceso es de extrema importancia, ya que de él dependerán todas las Políticas y Normas de Seguridad desarrolladas por la empresa.

1.5.1 Propietario

Todos, y cada uno, de los Recursos Informáticos y Activos de Información tienen que tener asignado un Propietario que actuará siempre por delegación de la Dirección de la empresa y será responsable de su protección.

En términos de Seguridad, el Propietario es el único que organizativamente tiene la responsabilidad de mantener operativos sus Recursos Informáticos y Activos de Información, determinar su criticidad y clasificación, establecerlos requerimientos de protección y conceder o eliminar derechos de acceso a los usuarios. Son responsabilidades del Propietario:

identificar Recursos Informáticos y Activos de Información de su propiedad; o no autorizar, salvo excepciones, el acceso público a sus Activos de Información (Artículo 9 de la LORTAD);

determinar los requerimientos de protección durante todas las etapas del ciclo de vida de los Activos de Información: creación, clasificación, calificación, manipulado, proceso automático, edición, reproducción, distribución, transporte, almacenaje, desclasificación y destrucción;

asignar y mantener la clasificación a los Activos de Información; o autorizar y mantener la vigencia de los accesos y el nivel de acceso de los usuarios, caso a caso, y siempre por razones de negocio;

impulsar las sanciones para los accesos no autorizados, de acuerdo con su naturaleza y con los daños ocasionados; o analizar y definir Activos de Información Sensibles; o analizar y definir Aplicaciones y Activos Críticos para el negocio; participar activamente en la creación del Plan de Recuperación y en sus pruebas periódicas;

analizar los resultados de las pruebas del Plan de Recuperación y, si fuera necesario, crear un Plan de Acción y revisar periódicamente su cumplimiento; especificar al Depositario los controles a establecer y las incidencias a comunicar; comprobar el cumplimiento de los controles requeridos al Depositario.

1.5.2 Depositario

El Depositario de los Recursos Informáticos y Activos de Información, generalmente la función de Sistemas de Información, es responsable de establecer y mantener los controles adecuados al nivel de protección requerido por el Propietario. Son responsabilidades del Depositario:

no permitir el acceso público a los Activos de Información, salvo excepciones autorizadas (Artículo 9 de la LORTAD);

proteger los Activos de Información según la clasificación asignada;

establecer y mantener los controles requeridos por el Propietario;

controlar los accesos de Usuarios autorizados por el Propietario; o comunicar al Propietario los nuevos controles técnicos que estén disponibles y cualquier desviación o anomalía detectada en los existentes;

informar a los Usuarios de los controles establecidos;

establecer los controles necesarios para impedir la instalación de productos sin licencia no autorizados por el fabricante;

realizar y coordinar el Plan de Recuperación y sus pruebas periódicas;

identificar Sistemas de Información Esenciales para los procesos de negocio.

1.5.3 Usuario

El Usuario es responsable de conocer el nivel de protección designado por el Propietario y cumplir con los controles establecidos por el Depositario, para todos los Recursos Informáticos y Activos de Información que maneje. Son responsabilidades del Usuario:

obtener la autorización formal del Propietario, antes de intentar acceder a cualquier Activo de Información;

informar al Propietario, cuando termine la necesidad de acceder a cualquier Activo de Información;

conocer la clasificación de los Activos de Información que maneja;

no divulgar información clasificada sin autorización del Propietario (Artículo 278 del nuevo Código Pena respecto a la revelación de secretos);

no intentar transgredir ningún control de protección establecido;

utilizar los Sistemas sólo para actividades de negocio de la empresa; o seguir las reglas establecidas para las contraseñas (passwords);

informar a Propietario y Depositario de cualquier anomalía de Seguridad detectada; no introducir personalmente ni utilizar ningún producto sin la correspondiente licencia autorización del fabricante.

2. Clasificación de Activos de Información

OBJETIVO

Definir un método de clasificación de los Activos de Información de la empresa, para su protección frente a pérdida, divulgación no autorizada o cualquier otra forma de uso indebido, ya sea de modo accidental o intencionado.

La información adopta muchas formas, tanto en los sistemas como fuera de ellos. Puede ser:

almacenada, en los sistemas o en medios portables;

transmitida, a través de redes o entre sistemas;

impresa o escrita, en papel y o hablada, en conversaciones.

Bajo el punto de vista de Seguridad, la protección adecuada debe ser aplicada a todas y cada una de las formas relacionadas con un Sistema de Información, es decir, a la tratada por medios informáticos.

Previamente a su clasificación, debe realizarse un inventario de Activos de Información asociados a cada Sistema de Información.

2.1 NIVELES DE CLASIFICACIÓN

Para clasificar un **Activo de Información**, pueden tenerse en cuenta los criterios definidos en los siguientes niveles :.información que podría ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la empresa o no. Denominación : Sin Clasificar o ninguna.

información que, sin poder ser publicada, puede ser conocida y utilizada por todos los empleados y algunos colaboradores externos autorizados, y cuya divulgación o uso no autorizados podría ocasionar pérdidas leves y asumibles por la empresa. Denominación : Uso Interno.

información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas, materiales o de imagen. Denominación : Confidencial.

información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la empresa, y que su divulgación o uso no autorizados podría ocasionar graves pérdidas materiales o de imagen. Denominación : Secreta o Reservada.

En adelante, se hablará de Información Clasificada refiriéndose exclusivamente a la descrita en los niveles 3 y 4 precedentes. Dada la posible coincidencia de denominaciones de clasificación, en distintas empresas, es recomendable calificarlas anteponiendo el nombre de la empresa o sus siglas registradas, para su diferenciación.

Sólo el Propietario de un Activo de Información puede asignar o cambiar el nivel de clasificación, con los requisitos previos siguientes:

asignarle una fecha de efectividad,

comunicárselo al Depositario y

realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación

2.2 MARCADO DE LA CLASIFICACIÓN

El nivel de clasificación, tiene que estar marcado en todas y cada una de las páginas de los Impresos que contengan información clasificada, incluyendo la carátula, siendo opcional el marcado en la cabecera o al pie de página, y siempre de forma que resulte fácilmente legible.

La información clasificada que aparezca en los Terminales de usuario, tiene que reflejar su nivel de clasificación, al menos, en la pantalla inicial y siempre que sea posible, en todas y cada una de las pantallas o estar permanentemente en la cabecera de pantalla.

Cada Medio de Almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, tiene que ser etiquetado con el más alto nivel de clasificación de la información que contenga. Los medios de almacenamiento NO desmontables no necesitan ser marcados con etiqueta de clasificación. La Información transmitida por medio de redes de comunicaciones (correo electrónico, teléfono, fax, etc.) debe ser marcada de acuerdo con el más alto nivel de clasificación de la información que contenga.

2.3 PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

Protección:

La principal regla de protección es que la información clasificada sea conocida o utilizada, sólo por personas autorizadas y siempre por razones del negocio de la empresa.

Todos los empleados tienen que tener suscrita con la empresa, o ser requeridos para ello, una Cláusula de Confidencialidad en la que firmen el compromiso de protección y no divulgación de la información clasificada que manejen por motivos de trabajo.

Guardar información clasificada en cualquier sistema o medio de almacenamiento supone:

tener los medios físicos y lógicos adecuados para protegerla;

no permitir su acceso público;

limitar el acceso a esta información.

2.3.1 Protección de Información Impresa

La información clasificada debe permanecer, en todo momento, lejos del alcance de empleados y personas que no tengan necesidad de conocer la información por motivo de su trabajo.

La información con clasificación Confidencial, debe guardarse bajo llave permanentemente, y durante su uso debe evitarse que pueda ser leída por nadie que no tenga necesidad de conocerla.

La información con el más alto nivel de clasificación tiene que permanecer guardada en una caja de seguridad y su utilización tiene que estar restringida a los momentos en los que nadie, que no esté autorizado, pueda verla o leerla.

El uso de cualquier dispositivo para generar salidas impresas que contengan información clasificada debe limitarse a aquellos que:

estén situados en áreas de Acceso Limitado o Restringido, o

tengan algún tipo de control de borrado de listados, o

sean de uso exclusivo del usuario (impresora personal).

Si ninguna de las opciones anteriores está disponible, se puede imprimir en cualquier otro dispositivo siempre que los listados sean recogidos personalmente por el usuario inmediatamente.

En cualquier caso, la creación de salidas impresas de información clasificada estará siempre bajo la responsabilidad y el control del usuario que genera la impresión.

2.3.2 Divulgación de Información Clasificada

La divulgación de información clasificada debe realizarse siempre sobre la base de la necesidad de conocerla por motivos de trabajo o tiene que ser autorizada, caso a caso, por el Propietario.

Cualquier divulgación a terceros, tiene que estar amparada por un Acuerdo de No Divulgación firmado, y con un período de validez que al expirar tiene que ser renovado, o suspendida la divulgación de la información clasificada.

El copiado y distribución de información clasificada debe tener la aprobación explícita del Propietario, quien puede reservarse el derecho de aprobar personalmente cada caso e incluso añadir la leyenda Prohibida la Reproducción o numerar las copias aprobadas, para su control.

Para una correcta divulgación, no debe transmitirse información clasificada a través de medios de comunicación inseguros, a menos que esté cifrada.

2.3.3 Transporte de Información Clasificada

Siempre que la información clasificada sea transportada dentro del ámbito de la empresa, bastará con ponerla en un sobre o contenedor cerrado y marcarlo con la clasificación más alta del contenido.

Si la información clasificada es enviada al exterior o por medio de correo ajeno a la empresa, el sobre o contenedor cerrado y marcado deberá ser introducido en otro sobre o contenedor cerrado y NO marcado. En el caso de la Información clasificada con el más alto nivel, tiene que incluirse, como medida de protección adicional, el acuse de recibo por parte del destinatario.

Siempre que la información clasificada sea enviada a través de redes de comunicaciones, propias o ajenas, debe considerarse la posibilidad de cifrado del Activo de Información, enviando la clave de descifrado por distinto conducto.

Durante los viajes, se deberá evitar el transporte de información clasificada. Si esto no fuera posible, el empleado deberá conservar la información en su poder durante todo el viaje, no debiendo dejarla desatendida en habitaciones de hotel, ni en vehículo alguno aunque esté cerrado, ni facturarla en aeropuertos o estaciones.

2.3. Destrucción de Información Clasificada

Cuando haya dejado de ser útil, la información clasificada debe ser destruida en la forma más adecuada al soporte que la contenga.

Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado o hacer ilegible la información contenida.

3. PROTECCIÓN FÍSICA

OBJETIVO

Evitar riesgos potenciales de ataque, pérdida, robo o daño a los Sistemas de Información de la empresa, accidentales o intencionados, que puedan ocasionar la interrupción, total o parcial, de las actividades de negocio. En este capítulo se pretende definir los medios a utilizar para la protección de las instalaciones donde están situados los Recursos Informáticos, incluyendo cualquier tipo de soporte físico, que contienen los Activos de Información de la empresa. También se hará referencia a aspectos no directamente relacionados con la Seguridad Informática (relativos a la seguridad de las personas o de las cosas) , pero sólo con el objeto de tenerlos en cuenta a la hora de planificar una instalación.

3.1 CARACTERÍSTICAS DE CONSTRUCCIÓN

Los edificios o instalaciones de una empresa donde estén, o vayan a estar, situados sus Sistemas de Información requieren unas características adicionales de protección física que deben ser consideradas antes de seleccionar su ubicación, teniendo en cuenta:

La posibilidad de daños por fuego, inundación, explosión, disturbios civiles, amenazas de vecindad, cercanía de instalaciones peligrosas (depósitos de combustible, aeropuertos, acuartelamientos, etc.),

cualquier otra forma de desastre natural o provocado. Adicionalmente,

Los elementos constructivos internos (puertas, paredes, suelos, etc.) deben cumplir el máximo nivel de protección exigido por la Norma Básica de Edificación.(NBE/CPI-91).

Estas instalaciones deben estar diseñadas de forma que no se faciliten indicaciones de su propósito ni se pueda identificar la localización de los Recursos informáticos.

Deben incluir zonas destinadas a carga y descarga de suministros, y su inspección de seguridad. Si todos los materiales no pueden ser inspeccionados en el momento, debe habilitarse una zona de consigna o depósito de materiales transeúntes hasta que puedan ser revisados.

Tienen que disponer de canalizaciones adecuadas para la conducción del cableado de comunicaciones y electricidad, para evitar ataques (sabotaje, fuego, roedores), interceptación o perturbaciones por fuentes de emisión próximas (radio, eléctricas, calor, etc.).

3.2 DISTRIBUCIÓN DE LAS ÁREAS

El edificio o instalaciones de la empresa pueden estar distribuido en varias áreas o zonas que, dependiendo de su utilización y los bienes contenidos, tienen que estar sometidas a una serie de controles de acceso.

Pueden distribuirse las instalaciones de acuerdo con los criterios y denominaciones siguientes:

Áreas Públicas Espacios en los que no hay ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.

Áreas Internas Espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización por motivos de negocio.Puede haber en ellos Recursos Informáticos, con un valor bajo.

Áreas de Acceso Limitado Espacios cuyo acceso está reservado a un grupo reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito. Pueden concentrarse en ellos Recursos Informáticos que, en conjunto, tienen un valor medio.

Áreas de Acceso Restringido Espacios cuyo acceso está reservado a un grupo muy reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por razones de negocio.

En ellos se concentran Recursos Informáticos que, en conjunto tienen un alto valor o contienen Activos de Información críticos para las actividades de negocio.

A las dos últimas (3 y 4) se les denomina Áreas Controladas.Tienen que permanecer cerradas, incluso cuando estén atendidas, y sus accesos controlados.

En las áreas Controladas, todos los empleados, y las personas ajenas a la empresa con autorización para acceder por razones de negocio, tienen que llevar permanentemente y en lugar visible un identificador:

Los empleados, al menos, con fotografía y nombre (legible a corta distancia).

Las restantes personas, al menos, el nombre (legible) y distintivo de la función que cumplen (ej.: visita, contratado, suministrador, etc.).

Los identificadores de los empleados con acceso a áreas Controladas de cualquier tipo, pueden tener la posibilidad de lectura por banda magnética o por cualquier otro medio, para facilitar el control de accesos y su registro.

Todo identificador, especialmente los que permitan el acceso a áreas Controladas, es personal y debe ser considerado como una contraseña de acceso físico y no compartirlo con nadie, para evitar verse envuelto en algún incidente de Seguridad no deseado.

Los suministros informáticos que sean peligrosos o combustibles tienen que ser almacenados a una distancia prudencial, no trasladarlos al área donde se encuentran los Recursos Informáticos hasta el momento de su utilización y retirarlos de la zona inmediatamente después de finalizar su uso.

En las áreas Controladas tiene que estar prohibido: comer, fumar y el consumo de bebidas alcohólicas o cualquier tipo de drogas. Las dos últimas están consideradas de alto riesgo potencial para la instalación, por lo que adicionalmente, debe impedirse la entrada a cualquier área Controlada a las personas de quien se sospeche el consumo, al margen de las acciones de tipo sancionador que hubiera que tomar.

A continuación, se establecen los requerimientos mínimos para los controles de acceso a cada tipo de área Controlada y su correspondiente gestión para que sean efectivos.

3.2.1 Áreas de Acceso Limitado (AAL)

La entrada a estas áreas tiene que ser desde un área Interna, nunca desde un área Pública.

Cada una de las áreas de Acceso Limitado tiene que tener identificado formalmente un responsable o Propietario, cuyas responsabilidades serán:

Aprobar y mantener actualizada, una lista o relación de las personas con autorización de acceso permanente.

Aunque no se requiere una revisión periódica formal de la lista de acceso, las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, tienen que ser eliminados de la relación de acceso en un tiempo razonable.

Aprobar accesos temporales a estas áreas. En este caso, la persona autorizada debe tener en cuenta que la autorización es para "una sola vez".

3.2.2 Áreas de Acceso Restringido (AAR)

La entrada a estas áreas tiene que ser desde un área Interna o un área de Acceso Limitado, nunca desde un área Pública, y no deben tener ventanas al exterior.

Tiene que tener barreras de aislamiento de suelo a techo, incluyendo el falso suelo y el falso techo, o bien detectores volumétricos de intrusos.

Cada una de las áreas de Acceso Restringido tiene que tener identificado formalmente un responsable o Propietario, cuyas responsabilidades serán:

aprobar y mantener actualizada, una lista o relación de las personas con autorización de acceso permanente.

Generalmente, porque el trabajo a realizar requiere su presencia física dentro del área.

La lista de acceso debe ser actualizada siempre que haya cambios que así lo aconsejen y revisada formalmente, al menos, cada seis meses. Las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, tienen que ser eliminados de la lista de acceso inmediatamente.

aprobar los accesos temporales a estas áreas, incluyendo los accesos del personal que, estando destinado en el área, accede fuera de su jornada laboral. En este caso, la persona autorizada debe tener en cuenta que la autorización es para "una sola vez". Las autorizaciones temporales deben contener:

nombre de quien autoriza, si no es el propietario,

el nombre del visitante autorizado,

razón social (si corresponde) o motivo,

fecha y hora del acceso,y la firma,

fecha y hora de salida, y la firma,

y tienen que ser guardadas como documentos auditables durante al menos un año.

El propósito de este registro es tener un archivo histórico de accesos, a utilizar en caso de investigación de incidente de Seguridad, pero en ningún caso es una herramienta de control de los empleados. El Propietario del área debe revisar, al menos mensualmente, que estos registros de acceso contienen la información descrita.

revisar y documentar que las salidas de emergencia tengan alarmas y sean audibles y/o visibles, en la propia sala y en el Centro de Control de Seguridad. Esta revisión debe ser realizada, al menos, anualmente y debe incluir la verificación de su correcto funcionamiento incluso con el

alumbrado de emergencia, cuando haya pérdida de suministro eléctrico. La documentación de las revisiones del funcionamiento de las alarmas debe guardarse como documento auditable.

3.2.2 Áreas de Acceso Restringido (AAR)

La entrada a estas áreas tiene que ser desde un área Interna o un área de Acceso Limitado, nunca desde un área Pública, y no deben tener ventanas al exterior.

Tiene que tener barreras de aislamiento de suelo a techo, incluyendo el falso suelo y el falso techo, o bien detectores volumétricos de intrusos.

Cada una de las áreas de Acceso Restringido tiene que tener identificado formalmente un responsable o Propietario, cuyas responsabilidades serán:

aprobar y mantener actualizada, una lista o relación de las personas con autorización de acceso permanente.

> Generalmente, porque el trabajo a realizar requiere su presencia física dentro del área. La lista de acceso debe ser actualizada siempre que haya cambios que así lo aconsejen y revisada formalmente, al menos, cada seis meses. Las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, tienen que ser eliminados de la lista de acceso inmediatamente.

aprobar los accesos temporales a estas áreas, incluyendo los accesos del personal que, estando destinado en el área, accede fuera de su jornada laboral. En este caso, la persona autorizada debe tener en cuenta que la autorización es para "una sola vez". Las autorizaciones temporales deben contener:

nombre de quien autoriza, si no es el propietario,

el nombre del visitante autorizado,

razón social (si corresponde) o motivo,

fecha y hora del acceso, y la firma,

fecha y hora de salida, y la firma,

> y tienen que ser guardadas como documentos auditables durante al menos un año. El propósito de este registro es tener un archivo histórico de accesos, a utilizar en caso de investigación de incidente de Seguridad, pero en ningún caso es una herramienta de control de los empleados. El Propietario del área debe revisar, al menos mensualmente, que estos registros de acceso contienen la información descrita.

revisar y documentar que las salidas de emergencia tengan alarmas y sean audibles y/o visibles, en la propia sala y en el Centro de Control de Seguridad. Esta revisión debe ser realizada, al menos, anualmente y debe incluir la verificación de su correcto funcionamiento incluso con el alumbrado de emergencia, cuando haya pérdida de suministro eléctrico. La documentación de las revisiones del funcionamiento de las alarmas debe guardarse como documento auditable.

3.2.3 Valoración de las áreas

Definición

Los requisitos de control de acceso físico deben basarse en el valor de los Sistemas de Información contenidos en cada área Controlada y en la importancia que las actividades de negocio suministradas por ellos.

El valor de un Sistema de Información puede obtenerse de acuerdo con los criterios siguientes:

Alto valor: sistemas corporativos grandes y medios.

Valor medio: pequeños sistemas corporativos y redes de área local (LAN).

Bajo valor: pequeños sistemas (PC) y terminales.

Aunque, para cada caso, deben considerarse otros aspectos tales como:

El coste y la necesidad de sustitución de los equipos acumulados en un área, o el impacto que podría ocasionar en la empresa la carencia prolongada de una actividad y la no disponibilidad de la información que suministra.

Esto lleva a definir como Sistemas Esenciales aquellos que contengan actividades críticas para el negocio de la empresa.

La valoración final debe ser realizada teniendo en cuenta todos los aspectos descritos para definir los requisitos de control de acceso y seleccionar el tipo de área Controlada, y deberían estar en consonancia con la tabla siguiente:

Tabla 1.Requisitos Mínimos de Control de Seguridad

SERVICIO	REQUISITOS	VALOR
	Alto	
Sistemas Esenciales para los Procesos de Negocio Medio MedioR	Bajo	Controles AA
	Bajo	
	Alto	Controles AAR
Sistemas No-Esenciales para el Negocio de la Empresa	Medio	Controles AAL
	Bajo	
Unidades de control de Teleproceso, independientemente del sistema que las soporte. Servidores, 'Bridges', 'Gateways' y 'Routers' de los		Controles

LAN y las Controles AAR herramientas que permitan visualizar el tráfico de las líneas (ej.: 'Sniffers', 'Spoofers', 'Trace tools', etc.)	AAR

NOTA: Estos controles no son aplicables a sistemas temporales dedicados a pruebas o demostraciones.

Para demostrar la correcta implantación y la efectividad del control de acceso físico, los propietarios de las áreas Controladas tienen que mantener actualizada, al menos, la documentación siguiente:

La identificación del área, el uso a que se destina, el nivel de información clasificada soportada, el valor de los equipos, la valoración del servicio y los requisitos de control requeridos.

La forma de comunicar a los usuarios de los servicios localizados en el área: el nivel de información clasificada soportada, las medidas de Seguridad adoptadas y los requisitos para su cumplimiento.

La valoración final, junto con todos los aspectos tenidos en cuenta para ello, tiene que ser documentada y guardada por el propietario del área Controlada como documentos auditables.

3.3 MEDIOS DE PROTECCIÓN

3.3.1 Sistemas de Control de Accesos

Los responsables de cualquier tipo de área Controlada tienen que mantener unos controles de acceso efectivos, en proporción a los recursos humanos y el valor de los activos a proteger, que pueden cumplirse de muy diversas formas (ej.: llaves, cierres con clave, sistema electrónico de control de accesos, guardas de seguridad, etc.), pero cualquiera que sea la forma elegida, tiene que cumplir con unos requisitos de auditabilidad mínimos (Artículo 9 de la LORTAD e instrucción 1/95 de la Agencia de Protección de Datos). Los objetivos son:

permitir el acceso únicamente a las personas autorizadas por el responsable o Propietario del área, y

registrar (quién, por dónde y cuándo) las entradas y/o salidas.

Para facilitar el control de los accesos a estas áreas, es recomendable la existencia de un único punto o puerta de acceso.

3.3.2 Sistemas de Detección

Las áreas Controladas deben contar con medios de detección de situaciones anómalas y previsibles para el área, tales como: puertas abiertas, acceso de intrusos, inundación, incendio o humos, etc.

Su objetivo es permitir un conocimiento inmediato y preciso del hecho y su localización, por lo que su actuación debe ser absolutamente fiable dentro de unos parámetros previamente establecidos. Ello exige unas revisiones de funcionamiento y un riguroso mantenimiento preventivo cuya periodicidad dependerá del sistema de detección y del tipo de área Controlada al que se aplique.

La detección de un hecho anómalo requiere la información necesaria para una reacción proporcionada. Dependiendo de la información suministrada por el medio de detección y de los parámetros previamente establecidos, antes de llegar a un estado de Alarma se puede pasar por un estado de Alerta, en el que algunos medios de reacción se van armando en previsión de su posible actuación.

Todos los medios de Detección pueden integrarse en un único sistema, preferentemente automático, que los gestione y que:

avise de la anomalía y su gravedad;

inicie acciones de corrección automáticas

proponga acciones manuales a realizar por personal entrenado para ello;

controle las actuaciones (qué, quién, cómo, dónde y cuándo).

Este sistema debe estar bajo vigilancia permanente y combinado con los servicios de mantenimiento, para los casos de mal funcionamiento de cualquier medio de detección.

Hay que subrayar que los sistemas de Detección deben funcionar incluso con el suministro eléctrico de emergencia.

3.3.3 Sistemas de Extinción de Incendios

En caso de incendio, su extinción puede realizarse con medios manuales o automáticos.

Los medios manuales se basan en extintores portátiles, mangueras, etc. Es importante resaltar que el elemento extintor localizado en un área debe ser el apropiado para el previsible tipo de incendio a declararse en ella. Cualquier medio de extinción puede ser excelente, utilizado en un área o más dañino que el propio fuego, si es usado en otra. Nunca debe emplearse un medio de extinción manual basado en agua donde pueda haber fuego eléctrico, por peligro de electrocución. No es aconsejable la intervención de personal no entrenado para ello. Siempre que se disponga de tiempo, hay que avisar a la Brigada Interior de Incendios (si la hubiera) o al Servicio de Bomberos.

Los medios automáticos se basan en la inundación del área mediante agua, CO_2 o compuestos halogenados.

El más recomendable es el basado en el agua, por su bajo coste y su nulo impacto en el entorno.

Los sistemas automáticos de extinción basados en el agua, deben tener un mecanismo de preacción que, en caso de llegar a un estado de Alerta o de Alarma, sustituye el aire de la conducción por agua. La actuación de estos sistemas de extinción debe estar combinada con la previa desconexión del suministro de energía eléctrica del área afectada.

Los restantes, aunque son efectivos, entrañan peligro para las personas y para el medio ambiente (capa de ozono, efecto invernadero, etc.), estando prohibidos por una u otra causa en la mayoría de los países firmantes del Protocolo de Montreal (control de uso de los CFC).

Las áreas Controladas deben contar con medios automáticos y manuales de extinción de incendios.

3.4 SUMINISTROS AUXILIARES

Recomendación

Es esencial la protección de las zonas que albergan los Suministros Auxiliares que dan servicio a los Sistemas de Información.

Sin una protección, equivalente a los Sistemas que soportan, serían mucho más sencillos de atacar y su destrucción o deterioro acarrearía graves interrupciones del servicio informático. Por tanto, deben estar ubicadas en un área de Acceso Limitado o Restringido, con los controles ya descritos para cada una de ellas.

3.4.1 Energía Eléctrica

Los Recursos Informáticos son sensibles a las variaciones de tensión y de frecuencia de la corriente eléctrica. Los requerimientos básicos para el suministro de energía eléctrica son dos: Calidad y Continuidad.

Relacionado con la Calidad, se puede destacar que:

Las variaciones de frecuencia deben corregirse con equipos estabilizadores que la mantengan dentro de los rangos establecidos por los fabricantes de los Recursos Informáticos a alimentar, aunque algunos Recursos Informáticos de nueva tecnología los llevan incluidos.

Las variaciones de tensión deben ser manejadas por un Sistema de Alimentación Ininterrumpida (SAI, en inglés UPS), de modo que se puedan prevenir los efectos de posibles microcortes. En relación con la continuidad del suministro eléctrico debe tenerse en cuenta que:

Las caídas de tensión pueden ser manejadas por un SAI (UPS), pero sólo por tiempo limitado (ya que el desgaste de sus acumuladores es muy rápido y su recarga muy lenta para utilizarlo en cortes sucesivos) y nunca como única alternativa.

Las soluciones habituales se basan en una de las siguientes, o en la combinación de varias de ellas:

conexión conmutada a dos compañías suministradoras; o conexión conmutada a dos estaciones transformadoras de la misma compañía, pero situadas en rutas de suministro diferente;

capacidad de transformación de corriente asegurada mediante equipos redundantes; equipos electrógenos, de combustión. Siempre que el volumen de las instalaciones informáticas así lo aconseje,

el suministro eléctrico debe ser independiente del general del edificio, y las tomas de tierra deben ser independientes de las generales del edificio, a suficiente distancia de ellas, correctamente instaladas y rigurosamente mantenidas.

3.4.2 Acondicionamiento de Aire

Con la evolución tecnológica de los fabricantes, existen en el mercado Recursos Informáticos que reducen (prácticamente eliminan) los tradicionales requerimientos de aire acondicionado.

Sin embargo, debido al parque informático existente y a su antigüedad media, se debe tener en cuenta las siguientes consideraciones:

Los Recursos Informáticos, especialmente los de las grandes instalaciones, generan calor que se hace necesario disipar a través de acondicionamiento de aire, que se encargan de mantener el ambiente con la temperatura y la humedad adecuadas, dentro de los límites indicados por los fabricantes.

La suficiente potencia y redundancia de estos equipos permitirá que trabajen desahogadamente y que las operaciones de mantenimiento sean sencillas y frecuentes.

Un elemento fundamental del sistema acondicionador de aire es el mecanismo de corte automático tras producirse una detección de incendio.

3.5 EMERGENCIA Y EVACUACIÓN

Tiene que haber implantado, de acuerdo con las Leyes y reglamentos en vigor (especialmente con la Norma NBE/CPI-91), un Plan de Emergencia y Evacuación de las instalaciones de la empresa.

Los objetivos de este Plan deben ser: o conocer los edificios y sus instalaciones, las áreas de posibles riesgos y los medios de protección disponibles;

evitar, o al menos minimizar, las causas de las emergencias;

garantizar la fiabilidad de los medios de protección;

tener informados de las medidas de protección a todos los ocupantes de las instalaciones;

disponer de personal organizado y adiestrado para las situaciones de emergencia;

hacer cumplir la vigente normativa de seguridad;

preparar la posible intervención de recursos externos (Policía, Bomberos, Ambulancias, etc.).

Hay que subrayar que la responsabilidad de confeccionar y mantener actualizado el Plan, recae en una función ajena a Sistemas de Información. No obstante, es necesaria su colaboración en el desarrollo de las medidas a tomar, relacionadas con las instalaciones informáticas, sus operaciones y las personas que trabajen en ellas.

3.6 MEDIOS DE ALMACENAMIENTO

Definición

En el concepto medios de almacenamiento están incluidos: cintas y cartuchos magnéticos y discos ópticos o magnéticos, ya sean desmontables o no.

El custodio (librarían) es la persona designada, y que ha aceptado la responsabilidad, para almacenar y controlar los medios de almacenamiento desmontables. El custodio tiene que poder controlar todos los movimientos de los medios de almacenamiento desmontables, a través de una aplicación o producto de su uso exclusivo.

En los casos en que la empresa tenga más de un Centro de Proceso de Datos, tiene que haber nombrado un custodio para cada uno de los centros.

En las redes de área local (LAN) y sistemas distribuidos, la información suele ser creada, accedida y almacenada en los discos magnéticos no desmontables de estaciones de trabajo y servidores. Siempre que en este tipo de sistemas exista información en medios de almacenamiento desmontables, tiene que ser nombrado un custodio por cada LAN o sistema.

Los conceptos de protección física, incluidos los traslados, y de inventario y reconciliación se refieren a los medios de almacenamiento desmontables. Sólo el tratamiento de la información residual hace referencia a cualquier tipo de medios de almacenamiento.

3.6.1 Protección Física

Todos los medios de almacenamiento bajo el control del custodio, deben estar situados en una AAL o AAR, dependiendo de la ubicación del sistema donde se procesen, y en una Zona Aislada cerrada a la que puede acceder exclusivamente el custodio.

Los medios de almacenamiento dedicados a salvaguardar la recuperación del sistema, y los servicios soportados, en el propio centro o en un centro alternativo, deben estar situados en otra Zona Aislada del mismo centro y en el centro alternativo.

Tiene que haber un control para evitar que los medios de almacenamiento desmontables sean montados o accedidos sin autorización. Ejemplos de este control son la utilización de etiquetas estándar (standard label), el uso restringido del proceso de 'BYPASS' de etiquetas estándar (BLP), el reconocimiento del volumen por el sistema, el intercambio de medios entre sistemas (en los cuales puede no estar definido), etc.

Los movimientos de medios de almacenamiento entre distintos centros, incluidos los dedicados a salvaguarda, tienen que ser registrados y guardados por el custodio de cada centro.

3.6.2 Protección Durante Traslados

Los medios de almacenamiento en tránsito tienen que ser protegidos, contra su pérdida, deterioro o uso indebido, desde que el custodio del centro origen los cede al transportista hasta que son recibidos por el custodio del centro de destino.

Durante su traslado, el soporte de almacenamiento y la información contenida tienen que asegurarse bajo los aspectos de:

Protección Física, para que no sean robados, sustituidos o dañados.

Protección Lógica, para que no sean leídos, copiados o modificados.

Para salvaguardar la confidencialidad, integridad y disponibilidad de la información transportada, tienen que usarse medios de transporte fiables, propios o de empresas solventes y responsables.

Para la información sensible o con el más alto nivel de clasificación, tienen que usarse contenedores cerrados, a prueba de penetración, y que sólo puedan ser abiertos por los custodios de los centros origen y destino. En casos excepcionales, habrá que fraccionar el envío en más de una entrega enviadas por rutas diferentes.

3.6.3 Inventario y Reconciliación

El custodio de medios de almacenamiento es responsable de:

implantar el procedimiento de control de inventario;

que se realice, al menos anualmente, el inventario de medios de almacenamiento y;

la correspondiente reconciliación, en caso de haber discrepancias.

Todos los medios de almacenamiento tienen que ser incluidos en el inventario, incluidos los volúmenes manejados por robots y los que estén sin grabar, por ser nuevos o borrados para su reutilización.

El proceso de inventario y reconciliación debe ser realizado por personas, al menos una, no directamente relacionadas con la responsabilidad de medios de almacenamiento, pero con la participación del custodio.

El proceso de inventario y reconciliación debe iniciarse partiendo de las cifras finales del anterior, incluyendo los nuevos volúmenes y los recibidos de otros centros, eliminando los volúmenes retirados o destruidos y los enviados a otros centros, y obteniendo la cifra final que será utilizada en el próximo inventario. Las discrepancias deben ser documentadas e iniciar el proceso de reconciliación.

La documentación relativa al proceso de inventario y reconciliación, incluyendo cualquier informe de discrepancias o incidentes, tiene que ser firmada por el custodio y por su línea de dirección o el propietario de la librería de medios de almacenamiento.

La documentación de soporte de los últimos inventarios y reconciliaciones tiene que ser guardada como documentos auditables.

3.7 IMPRESORAS

Definición

En este apartado, el término impresora se refiere a cualquier medio o dispositivo que pueda generar salidas impresas.

Se consideran dos tipos de impresoras, según sea su ubicación: las impresoras locales del Sistema, situadas en las áreas de Acceso Limitado/Restringido del propio Sistema y las impresoras remotas que no están situadas en las áreas dedicadas a los sistemas.

La responsabilidad de especificar las reglas de utilización de cada impresora es del propietario o responsable de ella.

El control de las salidas impresas es responsabilidad del usuario final que las envía a las impresoras.

El propietario del sistema o servicio no es responsable de que el propietario o el usuario de las impresoras remotas cumplan con los requerimientos de Seguridad descritos en este apartado.

Las salidas impresas de información clasificada tienen que ser protegidas contra accesos no autorizados.

Las impresoras remotas situadas en áreas Internas (NO situadas en AAL o AAR), tienen que tener alguno de los controles siguientes:

tener designado un responsable de entregar las salidas impresas al usuario final que las envió,o

estar directamente atendida por el usuario final,o

recoger los listados personalmente, e inmediatamente después de terminar la impresión, o

tener la posibilidad de borrado de listados pendientes de impresión.

Las impresoras locales o remotas situadas en AAL o AAR, no requieren ningún control adicional para imprimir información clasificada.

Si alguna AAL tiene una lista de acceso con un elevado número de personas, los controles adicionales del punto 1 son aplicables también al punto 2.

No puede haber impresoras remotas situadas en áreas Públicas

4. PROTECCIÓN LÓGICA

OBJETIVO

Proteger los Activos de Información de la empresa para que sean siempre utilizados de forma autorizada, y sólo por razones de negocio, y evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

El acceso de un usuario a los Sistemas de Información de la empresa tiene que estar basado, en cada caso, en una vigente necesidad de uso por razones del negocio de la propia la empresa.

Los usuarios tienen que estar informados de los aspectos siguientes:

Los Sistemas de la empresa sólo pueden ser usados para fines del negocio de la propia empresa.

El uso de los Sistemas para cualquier otro fin, no de negocio o personal, debe ser previamente aprobado por la Dirección.

El uso no autorizado de los Sistemas es una violación de los derechos de la empresa y se considera un abuso de confianza que debe ser sancionado.

Para ello, en la pantalla inicial de conexión debe aparecer una leyenda advirtiendo que "Los sistemas sólo pueden ser usados por razones de negocio u otros fines aprobados por la dirección", o cualquier otra equivalente.

Deben quedar sujetos a revisión en todo momento, por parte de la Dirección de la empresa, las actividades realizadas por los usuarios en los Sistemas de la propia empresa, u otros ajenos a ella para los que tenga autorización de uso, y la utilización en ambos casos de los medios de almacenamiento correspondientes.

4.1 Identificación de Usuarios

Objetivo

Aprobar el uso de cada Sistema y conocer a sus usuarios, asegurando que cada identificador de usuario es único y sólo puede ser asociado a una persona.

4.1.1 Identificador de Usuario

Es la clave que permite a un usuario acceder de forma individual a un Sistema de Información. Cada identificador de usuario tiene que estar asignado a una persona, que será responsable de las actividades realizadas con él.

Generalmente, un identificador de usuario (junto con la contraseña o cualquier otro método de autenticación) se asigna a una persona para facilitarle el acceso a un único Sistema de Información, debiendo adquirir otros identificadores para el uso de otros Sistemas. Esto provoca la multiplicidad de identificadores y contraseñas, tanto más cuanto mayor sea el número de Sistemas existentes en la empresa y la necesidad de su utilización. Para resolver este posible problema, es recomendable:

definir y utilizar una nomenclatura estándar en la creación de identificadores, de forma que un usuario tenga el mismo identificador en todos los Sistemas que necesite utilizar;

instalar un Sistema de Control de Accesos capaz de gestionar más de un Sistema de Información, con lo que el identificador de usuario (y la contraseña asociada) serían únicos y válidos para todos los Sistemas;

utilizar un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación una sola vez, en la primera conexión al sistema, pudiendo acceder posteriormente a cualquier otro Sistema o servicio por propagación o conversión a los distintos identificador de usuario y contraseña necesarios.

Adicionalmente, y dada la creciente necesidad de identificación (y autenticación) descritas, es posible dedicar un Sistema a las funciones de control de Seguridad, de modo que antes de permitir el acceso del usuario a cualquier Sistema de Información, se verifique una sola vez su identidad y autorizaciones de acceso. Este Sistema tendría que ser gestionado por el Administrador de Seguridad.

4.1.2 Identificador de Usuario Compartido

Hay casos en que un identificador de usuario proporciona acceso a determinadas funciones del sistema (ej.: operación del sistema) que tienen que ser utilizadas por un grupo de personas. En estos casos el identificador de usuario puede ser compartido por el grupo bajo las condiciones siguientes:

El identificador de usuario tiene que ser creado para el uso del grupo y no puede contener información individual, que el resto de los miembros del grupo no necesiten conocer.

Siempre que sea posible, la contraseña no debe ser compartida, para permitir la identificación de la persona que lo está utilizando.

Tiene que haber controles que eviten su uso no autorizado.

4.1.3 Autorización de Usuarios

El acceso de cada usuario a los sistemas de la empresa tiene que ser aprobado previamente por la Dirección. Tiene que haber definido un procedimiento, automático o manual, para autorizar la inclusión de nuevos identificadores de usuarios en los Sistemas y que incluya la notificación al director responsable del usuario.

4.1.4 Eliminación de Usuarios

En caso de terminación de la necesidad de uso por razones de negocio o abandono de la empresa, tiene que haber definido un procedimiento, automático o manual, para la eliminación de identificadores de usuarios del sistema. El director del usuario es responsable de comunicar a la Administración de Seguridad las condiciones de que son motivo de dicha eliminación.

El procedimiento debe incluir los controles para prevenir el acceso de un usuario a los Sistemas, inmediatamente después de la comunicación de su director.

Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro.

Revisión de Vigencia

Tiene que haber definido un proceso periódico para asegurar que no existen identificadores de usuario pertenecientes a empleados que hayan causado baja en la empresa.

Este proceso puede utilizar como base la comparación con alguna lista de empleados actualizada y servirá de salvaguarda en los casos en que el procedimiento de eliminación de usuarios no haya sido aplicado correctamente.

Todos los identificadores de usuario, de empleados no activos en la empresa , encontrados en este proceso tienen que ser eliminados del Sistema, junto con todos sus derechos de acceso concedidos, y su baja comunicada al director responsable del empleado.

Usuarios Inactivos

Un identificador de usuario sin uso puede ser una vía de acceso no autorizado al Sistema.

Tienen que establecerse controles para detectar identificadores de usuario que no hayan sido utilizados en los últimos 6 meses.

El proceso de detección de estos usuarios tiene que ser realizado, al menos mensualmente, y su acceso al Sistema, desactivado.

La desactivación tiene que ser comunicada al director responsable del empleado, advirtiéndole que en el plazo de un mes será eliminado el acceso al Sistema.

4.1.5 Revalidación Anual de Usuarios

Tiene que haber definido un procedimiento para la revalidación de usuarios, que debe ser realizado, al menos, anualmente.

Debe incluir el envío de la relación de usuarios a cada director que tiene empleados trabajando en el sistema, para que confirme si todos y cada uno ellos mantienen vigente la necesidad de uso por razones de negocio.

Las discrepancias deben ser comunicadas a la Administración de Seguridad para poder desactivar o eliminar a los usuarios.

4.2 AUTENTICACIÓN DE USUARIOS

Objetivo

Asegurar que un usuario es quien dice ser, cuando accede al Sistema.

En general, el proceso de autenticación de un usuario está basado en:

algo que sabe (contraseña);

algo que tiene (tarjeta, dispositivo, etc.);

algo que es (características biométricas).

La utilización de sólo uno de los métodos anteriores se denomina Autenticación Simple.

Cuando los controles de acceso tienen que ser especialmente restrictivos, pueden combinarse dos, o mas, métodos para eliminar, o al menos reducir, los riesgos de utilización no autorizada de un identificador de usuario. En este caso la denominación es Autenticación Reforzada.

La mayoría de los Sistemas de Información utilizan la Autenticación Simple por contraseña (password).

4.2.1 Contraseñas (Passwords)

La contraseña de acceso es, hoy por hoy, la principal protección porque verifica inequívocamente la identidad del usuario de un Sistema.

Deben considerarse información clasificada las contraseñas, o cualquier otro método utilizado, de autenticación de usuario de acuerdo con el máximo nivel de información clasificada que el usuario pueda utilizar en el Sistema.

Para la protección de los Activos de Información de la empresa y la protección del propio usuario, la contraseña:

tiene que ser secreta y no compartida con nadie,

no puede ser visualizada en pantalla mientras se teclea, y

no puede ser almacenada en claro (sin cifrar), en ningún tipo de Activo de Información.

Los sistemas operativos que incluyen algún Sistema de Control de Accesos, llevan rutinas de verificación de la calidad de la contraseña para evitar que pueda ser trivial o predecible. En cualquier caso, la contraseña debe disponer, como mínimo, de las características de calidad siguientes:

tener una longitud mínima de 6 caracteres; o tener al menos un carácter numérico y uno alfabético;

no empezar ni terminar con un número; o no tener mas de tres caracteres consecutivos idénticos, en cualquier posición, a los de una contraseña usada anteriormente;

no tener mas de dos caracteres iguales consecutivos;

ser cambiada, al menos, cada 60 días para usuarios generales y cada 30 días para usuarios que tengan algún tipo de privilegio o autoridad. Tiene que haber instalado un control que informe a los usuarios cuando su contraseña tiene que ser cambiada;

no ser reutilizada hasta después de, al menos, 12 cambios;

no contener el identificador de usuario, como parte de la contraseña.

En muchos casos, sistemas operativos, productos informáticos o aplicaciones traen una contraseña 'por defecto' para ser usada durante su instalación. Sin excepción, estas contraseñas tienen que ser cambiadas, si técnicamente es posible, durante la primera utilización o a la mayor brevedad posible, en caso contrario.

Si, por razones de negocio, una persona tiene que utilizar sistemas ajenos a la empresa, no debe utilizar en ellos la misma contraseña utilizada en los sistemas internos de la empresa.

Si el nivel de Seguridad es inferior en aquellos, podría ser detectada y utilizada sin autorización en los sistemas de la empresa.

Restauración de Contraseñas

Tiene que haber definido e implantado un proceso para asegurar la restauración o cambio de contraseña, por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona.

El proceso debe incluir la identificación positiva del solicitante o, en caso contrario, el envío de la nueva contraseña al director del usuario. Este proceso puede automatizarse para favorecer la gestión de la contraseña por el propio usuario o su director inmediato.

Tanto la solicitud como la respuesta deben realizarse a través de medios seguro.

4.2.2 Contraseñas de una Sola Vez

La contraseña de una sola vez consiste en un generador de contraseñas (dispositivo físico o lógico) externo al sistema, al que quiere conectarse el usuario, donde reside otro dispositivo (físico o lógico) sincronizado con el primero.

En el momento de la conexión, el usuario utiliza la contraseña que le genera el dispositivo físico (token) o lógico (ticket) que posee y que se compara con la que tiene el sistema. La contraseña utilizada cambia momentos después y si alguien la capturase, no podría utilizarla porque ya se habría producido una nueva contraseña.

4.3 ACTIVOS DE INFORMACIÓN DEL SISTEMA

Objetivo

. Asegurar la integridad de los Activos de Información del Sistema.

. Los Activos de Información que están relacionados con el propio Sistema y sus funciones o con los productos que lo componen, se denominan Activos de Información del Sistema y su protección es responsabilidad, generalmente, de la Función de Sistemas de Información.

. En este tipo de Activos cabe definir o destacar:

Los programas de control del sistema y sus mecanismos de control de acceso.

Los subsistemas, y productos soportados por Sistemas de Información, que formen parte del sistema operativo y sus funciones.

4.3.2 Activos Sensibles del Sistema

Esta denominación afecta a los Activos (datos y programas) que sean calificados sensibles por el departamento de Sistemas de Información.

Se entiende por Dato Sensible a cualquier Activo de Información cuya modificación o alteración inadecuada o no autorizada podría afectar gravemente a la integridad de los Sistemas de Información, sin ser prevenidas por los métodos habituales de control ni detectadas en un corto espacio de tiempo. Adicionalmente, este tipo de Activos tienen que ser actualizados a través de un programa o transacción del propio sistema y nunca pueden ser modificados o actualizados directamente. (ej.: Activos que contengan cualquier tipo de contraseñas de acceso al Sistema o a otros Activos de Información).

Un Programa Sensible es cualquier programa de utilidad o del propio sistema, cuya utilización no autorizada o inadecuada podría comprometer la integridad de los Sistemas de Información, sin poder ser prevenida ni detectada por los métodos habituales de control de Sistema. También se debe considerar sensible a cualquier programa de utilidad o del Sistema, que actualice Activos de Información definidos como datos sensibles. (ej.: cualquier programa de utilidad que analice el tráfico de red, ya sea local o extensa. Entre ellos los más conocidos por su denominación inglesa son: Spoofers, Sniffers, TraceTools, etc.). Un programa sensible sólo puede ser usado para los fines para los que fue creado, es decir, para el análisis, diagnóstico y resolución de problemas. Toda modificación, cambio o alteración de un Programa Sensible debe ser previamente autorizada.

Los Activos de Información Sensibles no pueden ser, en ningún caso, accedidos públicamente y no puede haber usuarios que tengan acceso permanente a ellos, incluyendo las copias de respaldo. Los accesos temporales tienen que estar plenamente justificados y aprobados caso a caso. Todas, y cada una, de las actividades de uso y acceso realizadas por los usuarios, tienen que ser registradas y revisadas. Los accesos temporales tienen que ser eliminados inmediatamente después de terminar la necesidad de uso.

4.4 ACTIVOS DE INFORMACIÓN DE USUARIO

Objetivo

Asegurar que cada Activo de Información de usuario está protegido, conforme a lo establecido por el Propietario, y que sólo tienen acceso los usuarios autorizados por él.

Los Activos de Información que pertenecen a un usuario o grupo de usuarios, a una aplicación o son parte de alguna de ellas, se consideran Activos de Información de Usuario y la responsabilidad de requerir los controles adecuados para su protección es de los propietarios en las restantes funciones de la empresa.

Para este tipo de Activos, tiene que establecerse una protección inicial por defecto que sólo permita su acceso al propietario del Activo. Todos los accesos concedidos posteriormente a otros usuarios tienen que estar explícitamente autorizados por el propietario, independientemente de la clasificación o calificación del Activo.

El propietario del Activo es responsable de establecer su protección y de los riesgos a que quede expuesto por una protección insuficiente. Tiene que asegurarse la integridad de todos los Activos de Información de Usuario.

4.4.1 Control de Acceso Público

Los Activos de Información de usuario no pueden tener ninguna opción que permita que sean accedidos públicamente.

Si un usuario considera que alguno de sus Activos tiene que ser accedido públicamente, debe:

certificar que el Activo no contiene información clasificada, y

comunicarlo al departamento de Sistemas de Información.

La función de Sistemas de Información registrará como Excepción todas estas solicitudes, advirtiendo al Propietario que su Activo va a ser accedido por todos los usuarios del sistema, incluidos usuarios externos si los hubiera.

Revisión Periódica

La función de Sistemas de Información tiene que comparar, al menos, mensualmente los Activos de Información de usuario que pueden ser accedidos públicamente con la lista de excepciones autorizadas. Si durante esta comparación se encuentra algún Activo de Información de usuario con acceso público y no registrado, se restaurará la protección inicial por defecto, permitiendo su acceso sólo al propietario.

La documentación relativa a estas revisiones debe ser guardada como documento auditable.

4.4.2 Activos Sensibles de Usuario

Esta denominación afecta a los Activos (datos y programas) que sean calificados como sensibles por el Propietario.

Se entiende por Dato Sensible a cualquier Activo de Información cuya modificación o alteración inadecuada o no autorizada, podría causar graves pérdidas financieras a la empresa sin poder ser prevenidas por los métodos habituales de control ni detectadas en un corto espacio de tiempo.

Adicionalmente, este tipo de Activos tienen que ser actualizados a través de un programa de aplicación o una transacción y nunca pueden ser modificados o actualizados directamente. (ej.: los

datos que contengan las cuentas a pagar de la empresa o los que contengan la información de pagos a empleados y que no tengan suficiente verificación manual posterior).

Un Programa Sensible es cualquier programa de aplicación cuyo uso, modificación o alteración inadecuados o no autorizados podría causar graves pérdidas financieras a la empresa y no pueden ser prevenidas ni detectadas por los métodos habituales de control de aplicaciones.

También se debe considerar sensible a cualquier programa de aplicación que actualice Activos de Información definidos como datos sensibles. (ej.: un programa que cree instrumentos financieros negociables y que no tenga suficiente verificación manual posterior).

Toda modificación, cambio o alteración de un Programa Sensible debe ser verificada por un programador independiente del que la realizó, comprobando que se ha efectuado de acuerdo con los requerimientos del Propietario. Los Activos de Información Sensibles no pueden ser, en ningún caso, accedidos públicamente y no puede haber usuarios que tengan acceso permanente a ellos, incluyendo las copias de respaldo.

Los accesos temporales tienen que ser plenamente justificados y todas, y cada una, de las actividades de acceso realizadas por los usuarios tienen que ser registradas y revisadas. Los accesos temporales tienen que ser eliminados inmediatamente después de determinar la necesidad de uso.

4.4.3 Protección en Desarrollo

La protección de los Activos de Información generados o tratados por una aplicación, debe comenzar a planificarse durante el análisis y el desarrollo (o modificación) y consolidarse durante las pruebas previas a su paso al sistema de producción.

Estos requerimientos son aplicables a los desarrollos realizados en la propia empresa o encargados a terceras partes, y deben permanecer vigentes en las posteriores modificaciones por mantenimiento de la aplicación. Simultáneamente con el desarrollo, o modificaciones de mantenimiento, deben crearse datos de prueba que verifiquen todas las alternativas de cada uno de los programas que componen la aplicación.

Nunca deben ser utilizados datos reales en pruebas, porque no se comprobarán todas las condiciones existentes en los programas y porque su utilización puede comprometer la confidencialidad, integridad y disponibilidad de los Activos reales de producción. Estos datos de prueba deben ser guardados durante la vida de la aplicación y actualizados cada vez que se realice alguna modificación en la aplicación que así lo aconseje.

Separación de los Sistemas de Desarrollo y Producción

Las actividades de desarrollo y prueba pueden causar cambios no deseados en Activos de Información de producción si comparten el mismo sistema o entorno operativo.

Para evitarlo, o al menos minimizarlo, hay que aislar, tanto como sea posible, los sistemas de desarrollo y prueba de los operacionales o de producción. Todos los desarrollos de aplicaciones, y sus posteriores modificaciones por mantenimiento, tienen que realizarse al margen del entorno operacional o de producción.

Dentro del área de gestión de cambios, el paso de aplicaciones desde el entorno de desarrollo y prueba al entorno operacional o de producción, no puede ser realizada por las mismas personas que desarrollan o mantienen las aplicaciones.

Uso del 'Estado Supervisor' (SVC)

Las aplicaciones de desarrollo local que utilicen llamadas al Supervisor tienen que estar documentadas y certificar que las 'SVC' no pueden ser usadas para evitar los controles de Seguridad del sistema.

Los propietarios de estas aplicaciones tienen que confirmar que las 'SVC' de su aplicación no pueden ser usadas para evitar los controles de Seguridad del sistema.

4.4.4 Protección de Terminales

Todo usuario es responsable de proteger el terminal que le ha sido asignado, y colaborar en la protección de cualquier otro terminal de la empresa, para evitar que sea robado o dañado (total o parcialmente), usada la información que contiene y utilizado el sistema al que está conectado. (Artículo 256 del nuevo Código Penal respecto al acceso no autorizado a terminales)

Durante la jornada laboral, en ausencias que excedan de un tiempo razonable (mas de 30 minutos), es necesario bloquear el terminal. Para ello utilizar la cerradura física (si la tiene) y guardar la llave en lugar seguro o utilizar productos de bloqueo y arranque mediante contraseña. Como protección adicional, si se trabaja en un despacho que disponga de cerradura, hay que cerrarlo con llave.

Al finalizar la jornada laboral, utilizar los mecanismos de bloqueo físicos o lógicos descritos en el punto anterior. Los despachos deben permanecer abiertos por razones de higiene (limpieza diaria) y Seguridad de las personas (si se produce un foco de incendio, inundación, etc. es necesario extinguirlo lo antes posible para evitar su propagación). Si el terminal es portátil, hay que guardarlo bajo llave o llevarlo consigo.

Durante los viajes (si se dispone de un terminal portátil), hay que usar mecanismos físicos o lógicos de bloqueo. No dejarlo nunca a la vista en el coche o en la habitación del hotel. No dejarlo al personal del hotel ni facturarlo como equipaje en aeropuertos o estaciones. Siempre que se pueda, el portátil debe permanecer en poder del empleado permanentemente.

Revisión Periódica

Los Coordinadores funcionales tienen que revisar, al menos mensualmente, que los terminales están convenientemente protegidos y que a través de ellos no pueden ser accedidos los Activos de Información contenidos en el terminal ni los Activos de Información contenidos en el Sistema o Servidor de una red de área local (LAN) al que pueda conectarse.

La documentación relativa a estas revisiones debe ser guardada como documento auditable.

4.4.5 Cifrado o Criptografiado

Cuando el acceso físico o lógico a los Activos de Información no pueda ser controlado o, por su especial sensibilidad o confidencialidad, requieran medidas adicionales de Seguridad, la información tiene que cifrarse de forma que quede ilegible y no pueda ser procesado por ningún usuario o persona no autorizada. (Artículo 400 del nuevo Código Penal respecto a la falsedad documental)

Un Activo de Información cifrado, para su almacenamiento o envío, mantiene el mismo nivel de clasificación y tiene que ser protegido como el Activo original.

Claves de Cifrado

La Clave de Cifrado (y descifrado) es una serie de caracteres usados para la codificación de los Activos, sin la cual no serán legibles ni podrán ser procesados.

Protección de las Claves de Cifrado

Para la protección de las claves de cifrado tienen que haber definidos e implantados los controles siguientes:

el uso de las claves debe estar restringido a personas

usuarios con necesidad de conocerlas por motivos de trabajo; o la gestión y distribución de las claves debe estar restringido a las personas o usuarios autorizados a realizar las funciones de cifrado;

la autorización de uso de las claves debe ser aprobada por el propietario de la información que se va a cifrar o descifrar;

el propietario de esta información puede delegar formalmente en el responsable del servicio de cifrado, si lo hubiera, la gestión y aprobación de las claves; el método usado para distribución de las claves tiene que poder asegurar que son recibidas por el destinatario, y sólo por él;

la clave de cifrado tiene que ser transmitida por un conducto distinto al del Activo, cuando éste se transmita cifrado;

cuando el cifrado y descifrado no se realice por medio de programas, los Recursos Informáticos tienen que estar protegidos en un área de Acceso Restringido (AAR).

Responsabilidades

Los propietarios de información cifrada, o los responsables del servicio de cifrado por delegación, tienen que asegurar que existen controles, para el cifrado y la protección de las claves, y son eficaces. Para poder demostrarlo deben guardar toda la documentación relativa al proceso y sus controles como documentos auditables.

4.4.6 Virus Informáticos y otros Códigos Dañinos

Son aquellos programas, rutinas o instrucciones desarrollados para provocar la destrucción o alteración de Activos de Información, en el Sistema. (Artículo 264.2 del nuevo Código Penal respecto a los daños informáticos)

Existen distintos tipos de código dañino y que, dependiendo de la característica que lo diferencia, se describen a continuación:

Virus Informáticos, el código que es capaz de generar copias de si mismo en programas distintos al que ocupa.

Gusanos (Worms), el código que absorbe recursos del Sistema, de forma creciente, hasta que lo bloquea por saturación.

Caballos de Troya (Trojan Horses), el programa de uso autorizado que contiene código dañino. Cuando este programa comienza a ejecutarse, el código dañino toma el control.

o Bombas Lógicas (Logic Bombs), el código que se ejecuta al producirse un hecho predeterminado, ej.: una determinada fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.

El más extendido es el Virus Informático que suele contener varias de las características descritas. A partir de ahora, por simplificar, se empleará la palabra Virus para referirse genéricamente a cualquier forma o tipo de código dañino.

Existen, en el mercado, programas Anti-Virus que detectan la presencia de virus y pueden eliminarlos. Estos programas van siendo actualizados de forma periódica, incorporando protección contra nuevos virus aparecidos. No obstante, siempre se estará expuesto a los virus que no hayan

sido incluidos en los programas anti-virus, pero el riesgo será mucho mayor si no utilizamos ningún método de prevención y/o eliminación.

Protección en LAN y PC

La Infección por virus se produce por la ejecución de un programa contaminado o el arranque del sistema desde un disco removible contaminado.

Se pueden dividir en dos grandes grupos:

virus de programa, que infectan a ficheros ejecutables (extensiones EXE, COM, SYS, OVL, OVR, etc.);

virus de sector de arranque, que contaminan el sector de arranque de discos removibles y discos fijos.

Para eliminar, o al menos minimizar, la infección por virus deben tenerse en cuenta las siguientes consideraciones:

establecer la prohibición de uso de productos sin licencia, no autorizados por la empresa o adquiridos de fuentes sin garantía;

verificar con programas anti-virus, antes de ser utilizado en el sistema, cualquier disco removible o fichero recibido que provenga de otro usuario, ya sea de la empresa o del exterior;

mantener un producto anti-virus residente de forma permanente en el sistema; actualizar el producto anti-virus utilizado, cada vez que se sepa que existe una versión más moderna que la que se está usando;

realizar periódicamente copias de respaldo;

proteger contra escritura todos los discos removibles.

Cualquier infección detectada en el transcurso de las verificaciones o revisiones descritas, tiene que ser notificada a la Dirección, para el aislamiento de los sistemas afectados, el análisis del virus y, si fuera necesario, su posterior inclusión en el anti-virus.

Adicionalmente, debe haber una protección para la conexión de sistemas a una red de área local (LAN), que garantice que ningún usuario pueda introducir programas o datos infectados en el servidor o en el sistema de cualquier otro usuario de la LAN.

Está prohibido, propagar conscientemente programas o datos infectados por virus dentro de, o desde, la empresa.

La responsabilidad de la utilización de anti-virus y la salvaguarda de las estaciones de trabajo (terminales) es del usuario final, pero el departamento de Sistemas de Información debe darle soporte para poder actualizar los programas anti-virus y canalizar las notificaciones de existencia de virus.

Protección en Sistemas Corporativos

La conexión de sistemas y redes a otros sistemas o redes puede suponer un grave riesgo para toda la red, los sistemas conectados a ella y los Activos de Información contenidos en los sistemas.

Deben controlarse todas las transferencias de Activos recibidas, verificando que ninguno de ellos es, o forma parte de, un virus conocido, con especial atención en los programas ejecutables.

Esto puede conseguirse instalando en los puntos de entrada (gateways) de la red y los sistemas filtros que seleccionen y supriman la transmisión de cualquier Activo o código dañino no deseados.

4.5 GESTIÓN DE LA AUTORIDAD DE SISTEMA

Autoridad de Sistema es la concedida a un usuario por asignación de atributos, privilegios o derechos de acceso que están asociados con la operativa del sistema y que son necesarios para realizar actividades de soporte, mantenimiento y operación del propio sistema.

Es conocido que los usuarios con este tipo de autoridad pueden usarla, de manera no apropiada, para evitar los controles de Seguridad del sistema y obtener algún beneficio. Esta situación tiene que ser considerada como un abuso de autoridad y sancionada.

Los accesos a los Activos de Información del Sistema, que no sean accesibles por un usuario general, tienen que estar basados en una necesidad de acceso válida y vigente, aprobada por el departamento de Sistemas de Información. Los usuarios cuyas responsabilidades incluyan el mantenimiento y soporte del sistema, están exentos de tener autorización escrita para acceder a ellos.

Los identificadores de usuario definidos para automatizar la operativa pueden ser considerados como parte integrante del sistema y asignados a un departamento de soporte y mantenimiento de sistemas, en vez de a un individuo. Los usuarios que puedan manejar este tipo de identificadores tienen que tener una necesidad de uso por razones de negocio válida y vigente, aprobada por el departamento de Sistemas de Información.

Los accesos a los Activos de Información del Sistema pueden ser implantados concediendo el acceso a un grupo de usuarios, siempre que cada acceso de un miembro del grupo pueda ser identificado individualmente. El departamento de Sistemas de Información tiene que tener definido e implantado un proceso, incluyendo revisiones periódicas, que asegure la permanente actualización de la lista de acceso y la eliminación de accesos cuando ya no sean necesarios.

Las actividades realizadas con Autoridad de Sistema tienen que estar específicamente autorizadas por la Dirección, por un proceso de control de cambios, o tienen que ser consistentes con la descripción del puesto de trabajo del usuario que la realiza. El departamento de Sistemas de Información tiene que asegurarse que los usuarios, que tienen esta autoridad, están informados de ello.

4.6 GESTIÓN DE LA AUTORIDAD DE ADMINISTRACIÓN DE SEGURIDAD

Objetivo

Asegurar que sólo los usuarios autorizados pueden añadir, modificar o eliminar funciones de administración de Seguridad del sistema.

Autoridad de Administración de Seguridad es la concedida a un usuario por asignación de atributos o privilegios que están asociados con el Sistema de Control de Acceso y que son necesarios para realizar las actividades de control y administración de Seguridad del propio Sistema.

Es conocido que los usuarios con este tipo de privilegios pueden usar, de manera no apropiada, la autoridad concedida para alterar algún componente de Sistema de Control de Accesos que redunde en su beneficio. Esta situación tiene que ser considerada como un abuso de autoridad y sancionada.

La Autoridad de Administración de Seguridad suele ser asignada a usuarios individuales, sin embargo puede también ser asignada a un usuario automático o a un grupo de usuarios, siempre que se cumplan las siguientes condiciones:

Cada acceso de un miembro del grupo pueda ser identificado individualmente.

Cada usuario perteneciente al grupo debe cumplir las reglas de este apartado, como si tuviera asignada la autoridad a su usuario individual.

Cada asignación a largo plazo (más de un mes) de esta autoridad a un usuario tiene que ser aprobada por escrito por la Dirección de Sistemas de Información y revalidada cada 12 meses.

Cada asignación a corto plazo (hasta un mes) de esta autoridad a un usuario tiene que ser aprobada por la Dirección de Sistemas de Información, o por un delegado formalmente (por escrito) designado. La aprobación tiene que ser anterior a la asignación de autoridad, aunque en asignaciones por emergencia se puede aprobar con carácter retroactivo.

Las actividades realizadas con Autoridad de Administración de Seguridad tienen que estar específicamente autorizadas por la Dirección, por un proceso de control de cambios, o tienen que ser consistentes con la descripción del puesto de trabajo del usuario que la realiza. La función de Sistemas de Información tiene que asegurarse que los usuarios, que tienen esta autoridad, están informados de ello.

Siempre que el Sistema de Control de Accesos lo permita, todas las actividades realizadas con esta autoridad tienen que ser registradas. El registro de estas actividades nunca debe ser desactivado. La función de Sistemas de Información tiene que definir:

el formato y el contenido de los documentos para la aprobación por escrito de la Autoridad de Administración de Seguridad;

un procedimiento para la asignación y aprobación de esta autoridad a corto plazo y en emergencia;

un procedimiento para la cancelación de esta autoridad cuando la necesidad de un usuario finaliza;

un procedimiento para detectar y corregir cualquier asignación de esta autoridad adquirida sin autorización, incluyendo el bloqueo del usuario que la ha obtenido.

4.7 REGISTROS DE INTENTOS DE ACCESO

Estos registros podrán ser creados siempre que exista un Sistema de Control de Accesos apropiado. Todos los registros especificados en esta sección tienen que ser guardados durante, al menos, un año.

Servirán de base para el análisis de cualquier incidente de Seguridad relacionado con los Sistemas de Información y como documentos a revisar en cualquier auditoría.

4.7.1 Registros de Acceso al Sistema

Tienen que ser registrados los accesos al sistema y los intentos de acceso inválidos.

Tienen que ser registrados los accesos al sistema y los intentos de acceso inválidos.

4.7.2 Registros de Acceso a Activos

Tienen que ser registrados los accesos a Activos de Información y los intentos de acceso inválidos.

4.7.3 Registros de Actividades

Las actividades realizadas usando la Autoridad de Sistema y la Autoridad de Administración de Seguridad tienen que ser registradas y su registro nunca puede ser desactivado.

4.8 INFORMES DE VIOLACIÓN DE ACCESO

Objetivo

Asegurar que los intentos de acceso no autorizado, al Sistema o a los Activos del sistema, pueden ser reconocidos como una violación, inmediatamente o después del consiguiente análisis.

4.8.1 Accesos Inválidos al Sistema

Tienen que establecerse controles para poder limitar el número de intentos fallidos de conexión al sistema, incluyendo el bloqueo del identificador de usuario, cuando se sobrepase el límite preestablecido por contraseña inválida.

El departamento de Sistemas de Información tiene que tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso al sistema, cuando sean solicitados.

Ataques Sistemáticos

El departamento de Sistemas de Información tiene que tener definido e implantado un proceso o controles que le permita detectar, gestionar e informar cuando se produzca un excesivo número de intentos de acceso inválidos al sistema o bloqueo sistemático de usuarios. Para evitar estimaciones subjetivas, cada sistema debe tener previamente fijado un límite a partir del cual se considera que está siendo atacado de forma sistemática.

4.8.2 Accesos Inválidos a Activos

El departamento de Sistemas de Información tiene que tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso a Activos, cuando sean solicitados por el Propietario.

5. CONEXIONES EXTERNAS

OBJETIVO

Mantener los niveles de protección de los Sistemas de Información cuando, de forma autorizada, sean accedidos por usuarios ajenos a la empresa o por empleados en conexión desde terminales no controlados por la empresa.

Las facilidades que la informática y las comunicaciones ofrecen a los usuarios, permiten ampliar cada vez más el campo de acción y la obtención de información conectándose a redes externas públicas que ofrecen servicios de proceso, red e información.

Al mismo tiempo, las empresas van estableciendo acuerdos de colaboración que implican la autorización de acceso y utilización de Recursos Informáticos y Activos de Información, bajo determinadas condiciones y en los que la conexión telemática es imprescindible.

Por todo lo anterior, se deduce que, al utilizar una red de comunicaciones externa y no controlada por la empresa, se están utilizando facilidades que pueden representar un riesgo para los Sistemas de Información de la empresa.

A continuación se incluye la descripción de algunos conceptos que van a ser usados en este capítulo, y al final del mismo un glosario de términos que puede ser de utilidad para su mejor comprensión.

CONEXIÓN EXTERNA es:

un acceso remoto a los Sistemas y Activos de Información internos, por empleados o por terceros, desde terminales que no están controlados por la empresa;

un acceso remoto a Sistemas o Activos de Información externos, por empleados, desde terminales controlados por la empresa;

una conexión entre un servicio interno y un servicio ajeno a la empresa.

El responsable que define la necesidad de establecer cualquiera de estos tipos de conexión, debe ser considerado como Propietario de la Conexión.

CONTROLADO POR LA EMPRESA:

Se dice del Recurso Informático, generalmente un terminal, que va a ser utilizado para establecer la conexión y que:

está en un edificio de la empresa, con los requisitos de control de acceso físico ya descritos;

está bajo el control directo de la dirección de la empresa, y

es usado para el desarrollo del negocio de la empresa.

GATEWAY

Es el entorno de proceso que permite la conexión, ya sea un Recurso Informático (hardware), o un Activo de Información (software o aplicación).

Normalmente, un 'gateway' suministra el enlace de comunicaciones inicial entre Sistemas internos y externos. El responsable del Sistema que suministra el servicio para el establecimiento de la conexión, debe ser considerado como Propietario del 'Gateway'.

ENLACE DE COMUNICACIONES

Es cualquier medio o tecnología que dé capacidad de teleproceso electrónico. Generalmente, una conexión física. NOTA: Los servicios de Voz y Fax no están incluidos en el ámbito de este capítulo.

5.1 RESPONSABILIDADES

Del Propietario de la Conexión

El propietario de una conexión externa es responsable de aprobar o denegar su establecimiento, de acuerdo con el informe del equipo revisor, y eliminar cualquier conexión cuando deje de ser necesaria para el negocio de la empresa o expire el plazo de tiempo para el que fue establecida. Adicionalmente, tiene que:

utilizar un 'gateway' existente que satisfaga las necesidades de la conexión requerida y cumplir con los procedimientos de autorización de acceso y revalidación periódica de uso existentes, o

solicitar la creación de un nuevo 'gateway', si ninguno de los existentes satisface las necesidades de la conexión requerida y asegurar que el propietario del 'gateway' recibe e incluye los procedimientos de autorización de acceso y revalidación periódica de uso.

Los procedimientos para autorizar el acceso de usuarios ajenos a la la empresa tienen que incluir la verificación de la vigente necesidad por razones de negocio y la revalidación de la autorización de acceso, al menos anualmente.

5.1.2 Del Propietario del 'Gateway'

El propietario de un 'gateway' es responsable de:

Implantar y mantener los controles de Seguridad del 'gateway';

Verificar los controles de acuerdo con lo descrito en el apartado de Certificación de la Conexión;

Aprobar la activación del 'gateway', después de asegurar el cumplimiento de los controles de Seguridad;

Mantener actualizada la relación de usuarios y accesos aprobados para cada 'gateway';

Registrar la información sobre el 'gateway', como ayuda a los propietarios de conexiones externas para decidir si existe un 'gateway' que cumpla sus requerimientos;

Implantar los procedimientos de autorización y revalidación de accesos suministrados por el Propietario de la conexión externa.

5.1.3 Del Usuario

Todo usuario, ya sea empleado o ajeno a la empresa, que utilice una Conexión Externa para:

Acceder a los sistemas o servicios internos de la empresa, desde un terminal no controlado por ella, o

Acceder a sistemas o servicios ajenos a la empresa, desde un terminal controlado por ella, tiene que cumplir con las normas especificas para este tipo de conexión, con los controles implantados y con cualquier otro procedimiento en uso aplicable al 'gateway' que se esté utilizando. (Artículos 197

y 278 del nuevo Código Penal respecto a la interceptación de correo electrónico y otras modalidades de telecomunicación)

Un usuario no puede conectarse simultáneamente a la red interna de la empresa y a otra red externa (no de la empresa). Esta conexión simultánea sólo puede ser utilizada excepcionalmente por razones de negocio y con la previa aprobación de la Dirección, para evitar que personas ajenas a la empresa puedan acceder a la red interna a través del terminal del usuario.

Un usuario, para conectarse a la red interna desde locales **NO** controlados por la empresa o a una red externa desde locales controlados por la empresa, tiene que:

tener la aprobación previa de la Dirección;

conectarse por un 'gateway' seguro, aprobado por la Dirección; o estar registrado en una Conexión Externa aprobada por la Dirección; o ser revalidada su participación, al menos, anualmente.

5.2 CERTIFICACIÓN DE LA CONEXIÓN

En una conexión externa, la revisión de certificación es una forma, generalmente aceptada, de verificar el cumplimiento de las normas y procedimientos de Seguridad implantados en la empresa.

5.2.1 Revisión Inicial

La revisión inicial y el subsiguiente informe de certificación de Seguridad, tiene que ser previa al establecimiento de la conexión.

Tienen que documentarse los procedimientos, resultados e incumplimientos de la revisión inicial, debiendo ser guardados por el propietario de la conexión externa mientras ésta persista.

Si la implantación de las medidas de Seguridad resultan inadecuadas o los controles no han sido aplicados correctamente, la conexión no puede ser activada hasta que, en posteriores revisiones, se alcance un total cumplimiento de los requerimientos de Seguridad exigidos.

Esta revisión termina con la certificación inicial de Seguridad y el establecimiento de la conexión externa.

5.2.2 Revisión Anual de Recertificación

Tiene que realizarse, al menos, anualmente una revisión de recertificación de características similares a la inicial.

El informe resultante y la documentación relativa a estas revisiones tienen que ser guardados por el propietario durante toda la vida de la conexión, junto a la de la revisión inicial.

Esta revisión termina con la recertificación de Seguridad y el mantenimiento de la conexión externa.

5.2.3 Suspensión de la Conexión

Después de la certificación inicial o de cualquiera de las anuales, pueden producirse cambios que afecten a la integridad de los controles. Tiene que establecerse un proceso para identificarlos e iniciar las pruebas de integridad adecuadas.

Cualquier riesgo detectado durante la vida de la conexión o en las revisiones periódicas tiene que ser identificado, documentado y valorado. Esta valoración tendrá como consecuencia un plan de acción para evitar o minimizarlos riesgos. Siempre que los riesgos no puedan ser resueltos inmediatamente, tiene que considerarse la posible Suspensión Temporal de la conexión externa, que sólo puede ser reactivada a través de un proceso de recertificación.

Tiene que establecerse un proceso para la Suspensión Definitiva de una conexión externa, cuando deja de ser necesaria o expira el plazo para el que fue establecida. Este proceso debe contener la inactivación de todos los usuarios incluidos en ella.

5.2.4 El Equipo Revisor

El equipo que certifica, tiene que estar compuesto por empleados, o asesores externos, con conocimientos técnicos del entorno y del proceso, pero pueden estar directamente relacionados con la conexión propuesta.

Su misión es intentar penetrar en el sistema o servicio, simulando el acceso de un usuario a través de la conexión externa.

El proceso de revisión, consiste en probar la efectividad de los procedimientos y controles utilizados para cumplir con los requisitos de Seguridad definidos. Para ello, pueden usarse técnicas tales como la inspección del diseño, el código fuente o los datos, los planes de prueba y sus resultados, y cualquier otra técnica que intente forzar los controles de Seguridad implantados, sin interrumpir el normal funcionamiento de los sistemas o servicios.

El equipo revisor tiene que emitir un informe para el propietario, con la certificación positiva de la conexión o las deficiencias encontradas y las acciones a tomar para ser resueltas.

5.3 AUTORIZACIONES DE ACCESO

La autorización de acceso tiene que ser verificada mediante un identificador de usuario y contraseña válidos, u otra identificación técnica que cumpla con las normas de Seguridad definidas por la empresa.

Una vez verificada la identidad del usuario que está accediendo, no debe haber restricciones para establecer la conexión, salvo las propias de la sesión o servicio con el que vaya a trabajar.

Tiene que haber definidos y establecidos controles para detectar y manejar los ataques sistemáticos contra el 'gateway'. Su Propietario debe ser informado cada vez que el número de accesos no autorizados sobrepase un límite previamente establecido en la instalación.

Conexiones DESDE el Exterior

Cualquier acceso, por razones de negocio de la empresa, a los sistemas o servicios internos a través de un 'gateway', tiene que ser justificado por el usuario, aprobado por la Dirección y registrado en la relación de autorizaciones del 'gateway', a través del cual se vaya a acceder. Todo ello, antes de ser establecida la conexión.

La utilización de esta modalidad, cada vez más frecuente, facilita a un usuario trabajar desde un terminal portátil o desde su propio domicilio.

Conexiones HACIA el Exterior

Un 'gateway' puede también ser usado para el acceso a sistemas o servicios ajenos a la empresa, desde terminales controlados por ella. Este tipo de conexión tiene que ser aprobada por la Dirección antes de ser puesta en funcionamiento y el usuario registrado en la relación de autorizaciones del 'gateway' a través del cual se conecte al exterior.

La utilización de esta modalidad facilita a un usuario la utilización, desde su puesto de trabajo, de redes, sistemas y servicios ajenos a la empresa, pero cada vez más necesarios.

Interconexión de Redes y Sistemas

En el caso de interconexión de redes, sistemas o aplicaciones, la identidad tiene que ser verificada en el momento de la conexión.

5.4 CONEXIÓN A REDES INSEGURAS

Cualquier usuario al conectarse a una red que sea, o se presuma que pueda ser, insegura para su simple uso o para comunicarse con organizaciones ajenas a la empresa, tiene que tener en cuenta que puede ser usada por usuarios ajenos a la empresa, en algunos casos de todo el mundo, y por tanto la información transmitida podrá ser leída, y posteriormente divulgada sin autorización, por muchos desconocidos y no todos desearán el beneficio de la empresa.

5.4.1 Riesgos en Redes Inseguras

No todos los usuarios utilizan estas conexiones para los fines previstos. Por ello, cualquier acceso desde o hacia una red externa puede representar un riesgo significativo para los Activos de Información de la empresa, debido a la posible:

Pérdida de integridad, por corrupción, de Activos de Información, como consecuencia del acceso no autorizado de usuarios a través de un punto de conexión a la red externa sin los controles adecuados.

Interceptación de información clasificada mientras transita por la red externa, pudiendo ser modificada o robada sin ser detectada por el emisor o el receptor.

Contaminación por virus, como consecuencia de la obtención de productos infectados procedentes de la red externa.

No observancia de las normas de Seguridad por parte de los usuarios correspondientes a algún acuerdo con terceros.

La protección contra estos riesgos exige una combinación de medidas de protección basadas en normas y procedimientos que los prevengan y en controles que los detecten y eviten (ej:. un Sistema Firewall).

5.4.2 Medidas de Protección

Al conectarse a cualquiera de estas redes inseguras desde un terminal controlado por la empresa, un usuario tiene que cumplir con unas elementales normas de ética y con las normas de Seguridad definidas por la empresa, entre las que cabe destacar las siguientes: o utilizar sólo los servicios a los que haya sido autorizado;

utilizar siempre su propia identidad, nunca una ajena;

no enviar ni almacenar información clasificada, a menos que esté cifrada;

no introducir ningún producto sin haber verificado previamente que cumple los requisitos legales de licencia y autorización del fabricante no obtener ningún producto para usarlo en la empresa, sin la previa autorización expresa de la Dirección, debiendo cumplir los requisitos legales de licencia y autorización del fabricante;

cualquier producto obtenido de redes externas no puede ser incorporado a los Sistemas de la empresa sin verificar previamente que no contiene ningún tipo de código dañino (virus);

no introducir ni obtener material ofensivo, amoral o no apropiado;

si existe un sistema de correo electrónico en la empresa, no usar este tipo de redes como correo interno entre empleados. Los usuarios no deben intentar comprobar la seguridad de la red interna, ni de ninguna red externa.

Las pruebas de integridad de la red están reservadas a una función específica designada por la empresa

5.4.3 Sistema Firewall (Cortafuegos)

Un Sistema Firewall consta de un conjunto de mecanismos, filtros de protocolo y dispositivos de control de accesos que manejan de forma segura la conexión entre una red protegida y una red insegura, tales como Internet o cualquier otra, incluyendo posibles sub-redes inseguras de la propia red interna de la empresa.

Este sistema protege las comunicaciones entre un usuario y una red externa, de la forma más transparente posible para el usuario, facilitándole al máximo los servicios que dicha red ofrece.

La mayoría de los sistema firewall están diseñados para asegurar el tráfico con la red Internet, debido a que representa la mayor fuente de información y de medios de comunicación con terceros, incluyendo: clientes, suministradores y cualquier otro tipo de personas que comparten intereses comunes.

Las fuentes de información se manejan a través del WWW (World Wide Web), que consiste en servidores WEB que contienen información, la mayor parte de uso público, y que son manejados por diversas organizaciones (suministradores, competidores, editores de normas, universidades, etc.).

Un Sistema Firewall está compuesto por:

un Sistema de Filtro de Paquetes (Packet Filter System) y

un Sistema de Servicios (Services System).

Sistema de Filtro de Paquetes

Constituye el frente primario entre la red propia y la red externa. Examina todos los paquetes de información intercambiados entre las dos redes y actúa según el tipo de paquete y las reglas configuradas por el administrador del sistema firewall.

Incluye una zona aislada de la red, llamada Zona Desmilitarizada (ZDM), que contiene información específicamente diseñada para ser compartida por usuarios de redes externas y es usada por:

servidores WEB externos,

servidores de FTP anónimo y

cualquier otro servidor que contenga información pública.

Los servicios de la propia red interna no pueden ser visibles a usuarios de redes externas, en cambio, los servicios que se facilitan al exterior (peticiones de información) son manejados por un servidor conectado a la zona aislada (ZDM).

Los paquetes que contienen direcciones IP desconocidas son rechazados.

Sistema de Servicios

El sistema de servicios procesa:

el correo electrónico (MAIL),

las noticias (NEWS),

las peticiones de transferencia de Activos (FTP)

las peticiones de Telnet (conexión a un servidor Internet).

Todo ello es manejado por un servidor de autenticación antes de que sea permitido el proceso.

Es recomendable que el Correo Electrónico sea manejado por un servidor de correo situado en la zona aislada (ZDM) y que dicho servidor no mantenga conexión con otro correo electrónico.

Las direcciones IP de la red interna tienen que cambiarse a direcciones IP del Firewall, antes de su salida al exterior, de forma que no sean visibles en el tráfico originado por el Firewall. Ocultar datos sobre la estructura interna (direcciones IP, identificaciones de nodos, etc.) ayuda a prevenir ataques del exterior.

5.5 TRANSFERENCIA DE ACTIVOS

La transmisión de mensajes, notas y documentos o datos y programas se considera una transferencia de Activos, siempre que se realice a través de un 'gateway' y desde o hacia un servicio interno de la empresa.

Tiene que haber un proceso que asegure la notificación de transmisiones no autorizadas al propietario del 'gateway' y poderlas prevenir y/o interrumpir.

Debe considerarse NO autorizada la transmisión de material ofensivo o amoral y los Activos que contengan virus, y adicionalmente el uso con fines fraudulentos de la red interna de la empresa. (Artículos 197, 256, 264.2 y 400 del nuevo Código Penal)

5.5.1 Correo Electrónico (Electronic Mail)

Es un medio de comunicación entre empleados, generalmente dentro del ámbito de la empresa, aunque también fuera de ella, que va adquiriendo un uso creciente. Este medio concebido para la transmisión de mensajes o notas, permite habitualmente la transmisión de todo tipo de Activos.

Además de las consideraciones generales de Seguridad a aplicar en cualquier Sistema de uso público, hay que tener en cuenta:

La posibilidad de interceptación de mensajes o notas, por lo que no debe incluirse en ellos información sensible que no esté cifrada.

La posible inclusión de virus o código dañino en los Activos de Información recibidos.

5.5.2 EDI (Electronic Data Interchange)

Es un estándar ISO para el Intercambio Electrónico de Datos en formato normalizado, entre los Sistemas de Información (y sus nodos de comunicaciones) de los participantes en transacciones comerciales.

Tiene que haber un acuerdo contractual, entre los participantes en el intercambio, sobre los derechos y deberes en la cesión y adquisición de información, así como los requisitos documentales y de prueba a ser utilizados en caso de litigio. El contrato debe contener aspectos tales como:

procedimientos a utilizar para las transacciones; o medios técnicos que intervendrán;

criterios de aceptación o rechazo de los documentos electrónicos;

responsabilidades del emisor de la Información;

responsabilidades del receptor de la Información, aspectos relacionados con la cesión de información sujeta a la Ley Orgánica de Regulación del Tratamiento Automático de Datos de carácter personal (Artículo 9 de la LORTAD).

Seguridad y Protección de Activos en EDI

Hay que establecer medios que garanticen el origen de la Información (mensaje EDI) y su integridad, es decir su no alteración. La protección de los mensajes EDI, se puede basar en:

el cifrado del contenido

> Puede realizarse con sistemas de cifrado disponibles en el mercado o con el propio que desarrollen los participantes en el EDI. Aporta la necesaria protección contra el acceso a mensajes EDI, ya sea accidental o deliberado, y que puede comprometer la confidencialidad de la información.

los comprobados de alteración

> Mecanismos que someten cada 'bit' transmitido a un proceso de cálculo, cuyo resultado es cifrado y también enviado. A la recepción del mensaje se repite el proceso de cálculo y se comparan los resultados, que deben coincidir. En caso contrario, significa que el mensaje ha sido alterado entre los dos elementos de proceso que hacen el cálculo.

la autenticación del contenido por firma digital

> Mecanismo de cifrado especial, basado en el algoritmo DSA (Digital Signature Algorithm), que añade una información para ser comprobada por el receptor.

el fechado y separado

> Cada mensaje debe ir fechado (fecha y hora) y separado de otros para evitar duplicidades.

el acuse de recibo

> Consiste en la devolución cifrada al emisor del mensaje recibido. Esto exige que el envío se haga con una clave y la recepción con otra, pero ambas conocidas por el emisor y el receptor.

la autenticación del contenido y la firma mediante Terceras Partes de Confianza (Trusted Third Parties)

> Organizaciones, públicas o privadas, que reciben una copia de la información, o partes de la misma, incluyendo acuses de recibo cifrados. Actúan como notarios de la transacción para posibles casos de repudio de los mensajes o acuerdos, con posterioridad a haberse recibido.

5.6 REGISTROS AUDITABLES

Hay que guardar registros auditables de las conexiones externas para, en caso de investigación de un incidente, poder determinar el uso de la conexión a los servicios internos de la empresa.

Para satisfacer este requerimiento, hay que crear un registro de la actividad de los 'gateways', que tiene que reflejar como mínimo para cada sesión establecida o acceso:

la fecha y hora,

identificación del origen (ej.: usuario del que proviene) y,

cuando la tecnología lo permite, tipo de acceso, destinatario y el nombre del Activo transferido.

Estos registros de actividades tienen que ser guardados, al menos, durante un año.

Adicionalmente, estos registros deben usarse para detectar ataques sistemáticos contra un 'gateway' y como respuesta a cualquier requerimiento del propietario del 'gateway' para su análisis.

5.7 ACUERDOS CON TERCEROS

Los Acuerdos con terceros que impliquen el acceso a Recursos Informáticos y Activos de Información de la empresa deben estar basados en un contrato formal que contenga las condiciones para cumplir las Normas de Seguridad de la empresa.

El contrato tiene que entrar en vigor antes de establecer la conexión y contemplar, al menos, los puntos siguientes:

Responsabilidades legales respecto a la información contemplada por leyes locales o nacionales (ej.: Artículos 9 y 27.2 de la LORTAD).

Acuerdos sobre copia y divulgación de información clasificada. o Medidas para asegurar la devolución de documentación y Activos de Información a la finalización del contrato. o Acuerdo para la investigación e informe de incidentes de Seguridad.

5.8 GLOSARIO DE TÉRMINOS

ROUTER:

Es un procesador de redes interconectadas que encamina paquetes de datos entre dos, o más, redes conectadas. El router IP encamina datagramas entre redes directamente conectadas o adyacentes.

GATEWAY:

Referido al contexto de la interconexión de redes se asimila a un Router

CORTAFUEGOS (FIREWALL):

Sistema (o router) diseñado para manejar de forma segura la conexión entre la red interna protegida y redes inseguras, públicas o sub-redes de la propia empresa. FTP: Protocolo de Transferencia de Activos (File Transfer Protocol). Método estándar para mover Activos de gran volumen usando Internet. FTP utiliza una arquitectura Cliente/Servidor en la que los usuarios pueden cargar y descargar Activos de Información.

SERVIDOR FTP ANÓNIMO (ANONYMOUS FTP SERVER):

Un sistema de Internet que permite el acceso público a Activos disponibles y su transferencia mediante FTP. IP: Protocolo Internet (Internet Protocol). El nivel de red requerido para conectarse con Internet.

DIRECCIÓN IP (IP ADDRESS)

La dirección física de un sistema Internet, expresada en el formato siguiente: xxxx.xxxx.xxxxx.xxxxx. Cada sistema tiene una única dirección IP.

TCP/IP:

Protocolo de Control de Transmisión/Protocolo Internet (Transmission Control Protocol/Internet Protocol). El protocolo de comunicaciones original de Internet y su espina dorsal. Es el más utilizado en el mundo de las comunicaciones y fue desarrollado bajo las directrices del Departamento de Defensa de los EE.UU.

INTERNET:

Red de comunicaciones mundial basada en el protocolo TCP/IP y originalmente fundada por la Agencia de Proyectos de Investigación Avanzados de la Defensa, la cual es parte del Departamento de Defensa de los EE.UU. Internet ha aceptado recientemente el tráfico de operaciones comerciales y de negocio.

TELNET:

Una aplicación que sirve para conectarse a Sistemas que, a su vez, están conectados a Internet. SERVIDOR TELNET: Aquel que permite el acceso Telnet.

WWW (WORLD WIDE WEB):

También llamado Web o W3. Una aplicación Internet cliente/servidor que permite a los usuarios navegar por Internet usando documentos de hipertexto. Requiere un cliente llamado popularmente 'browser'.

6. RECUPERACIÓN DE DESASTRES

OBJETIVO

Asegurar la continuidad de las aplicaciones críticas de negocio, en caso de desastre, total o parcial, del Sistema que las procesa.

6.1 IDENTIFICACIONES PREVIAS

6.1.1 Aplicaciones y Activos Críticos

Se denominan Aplicaciones y Activos Críticos a aquellos cuya falta de disponibilidad causaría graves dificultades en la continuidad de las actividades del negocio.

Cada PROPIETARIO de aplicación tiene que analizar el impacto que supondría para la empresa (ingresos que se dejarían de percibir, materiales que se estropearían, horas de trabajo que se perderían, etc.) la imposibilidad de procesar su aplicación. Deben tenerse en cuenta los siguientes factores:

Que puede ser crítica solamente una parte de la aplicación o sólo algún Activo de Información necesario para otra aplicación, en la misma Función o en otra diferente.

El tiempo máximo que podría subsistir la empresa sin procesar la aplicación.

Con estas bases, cada propietario tiene que seleccionar y proponer al Director Funcional las aplicaciones y Activos candidatos a ser nominados críticos, con la valoración de los costes asociados a la recuperación y las pérdidas potenciales, si no se recuperase.

La propuesta debe incluir una estimación de la periodicidad con que deberían efectuarse las copias de respaldo y la valoración de costes por el posible mantenimiento, en el departamento, de los datos de entrada a la aplicación durante el período existente entre dos copias de respaldo.

Cada Director Funcional, asistido por los propietarios, tiene que consolidarlas propuestas de los propietarios y determinar las aplicaciones y Activos candidatos, a ser propuestos como críticos, teniendo en cuenta:

los Activos de Información necesario para alguna aplicación de otras funciones;

el tiempo máximo que podría subsistir el negocio de la empresa sin el conjunto de aplicaciones y Activos críticos de la Función;y proponerlos en el Comité de Dirección, del que forma parte, incluyendo en la propuesta la valoración consolidada de costes de recuperación y pérdidas potenciales.

El Comité de Dirección tiene que analizar el impacto que podría ocasionar, en el negocio de la empresa, la carencia prolongada de Recursos, aplicaciones y Activos y la no disponibilidad de la información que suministran, teniendo en cuenta todos los aspectos necesarios para la recuperación.

Determinar formalmente qué aplicaciones y Activos son críticos para el negocio de la empresa, incluyendo la periodicidad con que se tienen que obtener las copias de respaldo, las fechas y cobertura de las pruebas y la información complementaria a mantener por las funciones.

Adicionalmente, deben valorarse las situaciones en las que podría ser declarada una emergencia y, en cada caso, quien está autorizado a declarar la situación de desastre, total o parcial.

La decisión final, y toda la documentación usada para ello, es de naturaleza confidencial y tiene que ser guardada como documento auditable y comunicada a las funciones y departamentos involucrados.

6.1.3 Centro Alternativo

A propuesta de la función de Sistemas de Información, el Comité de Dirección tiene que aprobar la alternativa más eficaz con el menor coste posible.

Si la empresa tiene capacidad para realizar la recuperación en un centro alternativo propio, debe tener prioridad esta opción, pero documentándolo en un acuerdo formal, que debe poder ser auditado.

La otra opción, es contratar un centro alternativo con alguna compañía especializada. Como regla general, el contrato contempla los conceptos de cargo siguientes:

por reserva de Recursos (capacidad, almacenamiento, etc.);

por prueba realizada y/o planificada;

por desastre real, en tiempo de ocupación;

por soporte técnico y asesoría.

Este último es el que puede considerarse como diferenciador entre un servicio de valor añadido y uno de simple disposición de los medios físicos para la recuperación.

En cualquiera de las dos opciones, el centro alternativo, propio o externo, tiene que cumplir como mínimo los requisitos de Seguridad física existentes para el centro origen.

Al margen de las consideraciones anteriores, el contrato, en cualquier caso, debe garantizar la disponibilidad del centro alternativo y la realización de las pruebas periódicas de recuperación en las fechas predeterminadas. Antes de la firma del contrato debe revisarse el centro alternativo, verificar qué es adecuado y qué cubre las necesidades de recuperación previstas por la empresa. El contrato y el informe de la revisión previa deben guardarse como documentos auditables.

6.1.4 Revalidación Periódica

Todo el proceso de identificación descrito, tiene que ser repetido siempre que existan modificaciones en los servicios suministrados por Sistemas de Información, que así lo aconsejen, o al menos anualmente. El momento recomendado para esta revalidación es durante el análisis de los resultados de una prueba de recuperación.

6.2 COPIAS DE RESPALDO (BACKUPS)

Determinada su periodicidad, debe crearse un procedimiento que contenga los detalles de obtención de estas copias, de acuerdo con el fin para el que son creadas, recuperación parcial o total, y el destino, el propio centro o el centro alternativo.

La obtención de un juego de copias de respaldo, puede realizarse:

Sobre medios de almacenamiento desmontables, lo que implica su traslado al centro de almacenamiento alternativo a la mayor brevedad posible y planificar el mantenimiento de, al menos, tres juegos de copias de respaldo para asegurar, que al menos un juego permanece siempre en el centro de almacenamiento alternativo de forma rotatoria.

En el traslado tiene que depositarse el nuevo juego de copias y recoger para su reproceso el más antiguo de los existentes.

Mediante la transferencia electrónica de los Activos de Información al centro de almacenamiento alternativo, donde se cuenta con los dispositivos de grabación y lectura adecuados. Esta opción resuelve los problemas derivados del transporte, aunque hay que tener en cuenta la cantidad de Activos de Información y la distancia como nuevos parámetros que pueden ser causa de problemas e incremento de costes.

Es recomendable planificar la obtención de las copias de respaldo al terminar todos los procesos diarios, con lo que todos los Activos de Información estarán actualizados y al mismo nivel.

6.2.1 Almacenamiento en el Centro Alternativo

En el caso en que las copias de respaldo no se guarden en un centro de almacenamiento alternativo, tiene que habilitarse una Zona Aislada, controlada por un custodio, como almacenamiento en el centro alternativo, para trasladar y guardar los juegos de copias de respaldo, para la recuperación en el centro alternativo. Las características de protección y control de acceso físico tienen que ser las mismas que en la Zona Aislada original.

Si no existe un custodio de la empresa en el centro alternativo, los juegos de copias tienen que permanecer cerrados, en los contenedores que son trasladados, y no accesibles por ninguna persona ajena a la empresa.

6.2.2 Almacenamiento en el Propio Centro

Tiene que habilitarse una Zona Aislada, controlada por un custodio, como almacenamiento alternativo en el propio centro, para trasladar y guardar los juegos de copias de respaldo para la recuperación en el propio centro. Las características de protección y control de acceso físico tienen que ser las mismas que en la Zona Aislada original.

6.2.3 Respaldo Funcional Complementario

Durante el período de tiempo existente entre dos copias de respaldo consecutivas, las funciones de la empresa siguen introduciendo datos en los Activos de Información o modificando programas de las aplicaciones, si unos u otros han sido declarados críticos para la recuperación del negocio, todas las modificaciones realizadas tienen que ser retenidas por la función hasta que otra copia de respaldo las incluya.

Si se declara una situación de desastre, una vez restaurada la copia de respaldo al sistema alternativo, todos los Activos incluidos en el Sistema con posterioridad a la obtención de la copia de respaldo, tienen que ser recuperados para tener en el Sistema la situación en el momento del desastre.

Este plan complementario tiene que ser realizado por cada uno de los propietarios de aplicaciones o Activos críticos y consolidado a nivel función, con la participación del coordinador funcional de Seguridad.

Tiene que prevenirse que un desastre afecte a la función y pueda deteriorar o destruir totalmente esta información complementaria.

6.3 PRUEBAS DE CONTINUIDAD

La Función de Sistemas de Información tiene que tener analizadas las alternativas, en lo referente a capacidad de proceso y almacenamiento, para determinar en qué supuestos se realizaría la recuperación en el propio centro, ya que esta opción debe ser prioritaria, siempre que sea factible.

Entre las actividades planificadas para la recuperación en caso de desastre, tienen que incluirse las pruebas de continuidad de operaciones en el propio centro, en el centro alternativo, la revisión de los procedimientos y su correspondiente actualización.

Tiene que planificarse, al menos, una prueba de continuidad al año, de tal forma que pueda garantizarse la recuperación en caso de desastre.

Una declaración ficticia de desastre, parcial o total, tiene que desencadenar la realización de una prueba de recuperación planificada, en el propio centro o en el centro alternativo.

La función de Sistemas de Información tiene que nombrar formalmente un responsable de, al menos, las actividades siguientes:

coordinar con la dirección de las funciones la realización de las Pruebas de Recuperación;

recabar la conformidad de los propietarios con los resultados de las Pruebas de Recuperación;

emitir los informes de los resultados de las Pruebas de Recuperación, y actualizar los Procedimientos de Recuperación, siempre que haya cambios que así lo aconsejen, al menos una vez al año.

Durante las pruebas no puede usarse ningún Activo de Información que no esté contenido en las copias de respaldo. Cualquier utilización adicional, aunque sea encaminada a la finalización de las pruebas, tiene que ser incluida en el informe como incidente y la prueba declarada no satisfactoria.

Todos los incidentes detectados durante las pruebas tienen que quedar reflejados en el informe. Los propietarios o funciones afectadas tienen que tomar las medidas necesarias para corregirlos, mediante un plan de acción. Si algún incidente, habido en el transcurso de las pruebas, impide la recuperación, la prueba tiene que ser declarada no satisfactoria y repetida antes de 3 meses.

Una prueba se considera terminada de forma satisfactoria, cuando se han podido recuperar el sistema y la información al mismo nivel que tenían en el momento de la declaración (ficticia) de desastre.

6.3.1 En el Centro Alternativo

Durante las pruebas de recuperación se pueden diferenciar tres fases:

Fase de PREPARACIÓN, que no debe durar más de 24 horas desde la declaración de desastre, e incluye las actividades siguientes:

Traslado al centro alternativo.

Recuperar las copias de respaldo más recientes.

Volcar las copias de respaldo.

Recuperar el sistema operativo.

Recuperar las aplicaciones y Activos críticos.

Verificar el nivel del servicio recuperado. Al término de esta primera fase, el servicio debe reflejar la misma situación que cuando se obtuvieron las copias de respaldo.

Fase de EJECUCIÓN, cuya duración estará en función de la periodicidad de la obtención de las copias de respaldo (cuanto mayor sea el período entre dos copias, más tiempo tendrá que

emplearse en la introducción de la información de las funciones), e incluye las actividades siguientes:

Comenzar las actividades de continuidad. o Introducir la información complementaria de las funciones.

Procesar las aplicaciones críticas hasta la recuperación total. Anotar los incidentes ocurridos.

Comprobar los resultados con las funciones (propietarios). Al término de esta fase, el servicio debe reflejar la situación que tenía cuando se declaró la situación de desastre.

Fase de INFORMACIÓN, en caso de que la prueba resulte satisfactoria, su duración no debe sobrepasar las 48 horas. Esta última fase contiene las actividades siguientes: Solicitar conformidad formal (por escrito) de las pruebas, a los propietarios. Realizar y distribuir el informe de las pruebas, a propietarios y directores funcionales. Actualizar los procedimientos de recuperación. Si los resultados de la prueba son satisfactorios, la recuperación termina aquí. En caso contrario, se tiene que continuar con las actividades siguientes:

Crear los planes de acción para corregir los incidentes, fijando la fecha de repetición de la prueba.

Realizar el seguimiento de los planes de acción e informar a la Dirección.

Repetir la prueba antes de tres meses.

> Hasta la repetición de la prueba, la instalación debe mantenerse en situación de emergencia.

6.3.2 En el Propio Centro

Excepto el traslado al centro alternativo, deben realizarse las mismas actividades que en el apartado anterior. La recuperación en el propio centro, implica la asignación de Recursos Informáticos al servicio esencial siniestrado, y por tanto la suspensión o la reducción de capacidad de otro servicio no esencial para el negocio de la empresa.

Generalmente, esto supone que el servicio recuperado funcione también degradado, al no tener la misma capacidad de proceso y almacenamiento.

6.3.3 Recuperación del Centro Siniestrado

Tiene que realizarse un análisis y una valoración de las posibles pérdidas de bienes muebles e inmuebles, Recursos Informáticos y Activos de Información, en caso de un desastre real.

La sustitución temporal está contemplada en apartados anteriores con la recuperación de los sistemas y servicios esenciales.

En este apartado se tiene que considerar la reparación del centro siniestrado, o su sustitución por otro de nueva construcción, con los costes asociados, el plazo de tiempo requerido en una situación de emergencia, que no debería sobrepasar los seis meses para la total recuperación, y el retorno al centro origen. A efectos de valoración, tienen que considerarse ambas alternativas de desastre, el total y el parcial.

Este plan es el único que teniendo que estar realizado y actualizado, no debe ser probado por el elevado coste que representaría.

5.5 TRANSFERENCIA DE ACTIVOS

La transmisión de mensajes, notas y documentos o datos y programas se considera una transferencia de Activos, siempre que se realice a través de un 'gateway' y desde o hacia un servicio interno de la empresa.

Tiene que haber un proceso que asegure la notificación de transmisiones no autorizadas al propietario del 'gateway' y poderlas prevenir y/o interrumpir.

Debe considerarse NO autorizada la transmisión de material ofensivo o amoral y los Activos que contengan virus, y adicionalmente el uso con fines fraudulentos de la red interna de la empresa. (Artículos 197, 256, 264.2 y 400 del nuevo Código Penal)

6.4 SITUACIÓN DE DESASTRE

Cuando un problema, de cualquier índole o naturaleza, paraliza, total o parcialmente, los servicios informáticos de la empresa, el primer paso tiene que ser el análisis de la situación y sus posibles soluciones alternativas. Las soluciones tienen que ser evaluadas e informadas a la Dirección, quien procederá a declarar, o no, la situación de desastre:

Parcial, a recuperar en el propio centro, con indicación de los sistemas esenciales a recuperar, o

Total, a recuperar en el centro alternativo. En ambos casos, la situación de desastre debe estar declarada antes de 24 horas desde que se produjo el evento, y desencadenar los mecanismos planificados para la continuidad de las operaciones.

6.4.1 Continuidad de Operaciones

Una vez declarada la situación de desastre, total o parcial, tienen que desencadenarse las actividades de recuperación de los sistemas esenciales siniestrados.

Las actividades a realizar son las mismas que están descritas en el apartado correspondiente a las pruebas planificadas.

En casos de desastre total y recuperación en el centro alternativo, tiene que considerarse, adicionalmente, el retorno al centro origen, reparado o sustituido, antes de 6 meses.

Es necesario resaltar que la diferencia sustancial con una prueba, es que, por tratarse de un desastre real, un resultado no satisfactorio en la recuperación supondría pérdidas de Recursos y Activos con consecuencias económicas que en algunos casos pueden ser irrecuperables.

7. PROGRAMAS PREPARATORIOS Y DE CONTROL

OBJETIVOS Comprobar que los empleados reciben periódicamente la formación de Seguridad adecuada. Verificar periódicamente que los controles de Seguridad funcionan correctamente y para los fines que fueron creados. Adicionalmente, verificar que han sido tenidas en cuenta las recomendaciones del informe del anterior diagnóstico de Seguridad, e implantadas las acciones necesarias para corregir los riesgos reales o potenciales descritos.

Para ello se pueden definir unos indicadores que cubran todo el ámbito de la Seguridad de la empresa y que, de acuerdo con su valoración, nos vayan definiendo el nivel de implantación y los riesgos identificados.

A continuación se definen los indicadores y los valores que se alcanzan en cada uno de ellos, de acuerdo con los detalles que se describirán más adelante, en los distintos apartados de este capítulo.

Tabla 2. Indicadores Clave de Control de Seguridad

Indicadores	Máximos puntos	Pleno Cumpl.	Control	Bajo Riesgo
1. Organización de Seguridad	10	9	9	7
2.Formación de Empleados	15	14	13	10
3a.Integridad de Sistemas	20	19	18	14
3b.Inventario y Clasificación	20	19	18	14
4. Revisiones y Auditorías	20	19	18	14
5. Recuperación de Desastres	20	19	18	14
6. Otras Actividades	15	15	14	11
TOTAL	100	95	90	70

La función de Sistemas de Información tiene que realizar las actividades relativas al indicador 3a, mientras que las restantes funciones lo harán con el indicador 3b.

De acuerdo con la puntuación obtenida sumando la de los 6 indicadores, se obtiene una puntuación global que valora el nivel de implantación y cumplimiento, de acuerdo con la tabla siguiente y obteniendo un valor final entre 1 y 5.

Tabla 3. Valoración según Indicadores Clave de Control

Puntos	Valoración Final	Valor Obtenidos
> = 95	Pleno Cumplimiento	1

> = 90	Controlado	2
> = 70	Bajo Riesgo	3
> = 60	Riesgo Medio	4
< 60	Alto Riesgo	5

7.1 ORGANIZACIÓN DE SEGURIDAD

Deben planificarse anualmente actividades de formación específica de Seguridad para todos aquellos empleados con dedicación al área de Seguridad Informática. El objetivo es asegurarse que existe una organización de Seguridad y que es efectiva.

Coordinadores de Seguridad.

Administradores centrales.

Administradores locales.

Empleados con Autoridad de Sistema.

Empleados con Autoridad de Administración del Sistema.

El porcentaje de empleados dedicados a Seguridad en la Función cuya formación en el área de Seguridad ha sido actualizada o mejorada en los últimos doce meses frente al total de empleados dedicados a Seguridad en la Función, nos dará la base para la obtención de los puntos correspondientes a este apartado, sobre el máximo definido.

7.2 FORMACIÓN DE EMPLEADOS

Deben ser planificadas anualmente sesiones de formación de Seguridad para los empleados, que pueden realizarse como sesión específica o incluirlas en reuniones que cubran otras áreas de negocio. El objetivo es la formación de todos los empleados al menos una vez al año.

Debe obtenerse una relación que contenga la fecha, el temario y la firma de los asistentes, y guardarla como documento auditable. Las sesiones formales pueden ser sustituidas por cualquier tipo de herramienta de formación en el sistema (on-line), siempre que cumpla con los requisitos de auditabilidad especificados. No debe aceptarse la formación por memorándums.

El porcentaje de empleados formados en los últimos doce meses frente al total de empleados de la Función nos dará la base para obtener los puntos correspondientes a este apartado, sobre el máximo definido.

7.3 A PRUEBAS DE INTEGRIDAD DE SISTEMAS

Deben ser planificadas anualmente pruebas de integridad de los sistemas, seleccionándolos con criterios de importancia. La selección debe incluir los sistemas esenciales para los procesos de la empresa, los que tengan información clasificada o con el mayor número de usuarios.

Una prueba se considera satisfactoria cuando NO se ha podido:

Adquirir autoridad de sistema.

Adquirir autoridad de administración del sistema.

Eludir cualquier control de Seguridad del sistema.

Acceder a información clasificada, por cualquier medio legítimo.

Cuando cualquiera de los puntos anteriores puede ser realizado, la prueba es insatisfactoria y el sistema se considera Penetrado.

Una prueba insatisfactoria, con riesgos detectados, tiene que ser repetida no más tarde de 30 días.

Para realizar las pruebas deben suministrarse, al menos, las facilidades siguientes: El uso de un terminal conectado al sistema a probar.

Un identificador de usuario, y su contraseña, para poder conectarse al sistema. Este usuario no debe tener ningún tipo de privilegios o derechos especiales de acceso a Activos de Información.

Una relación de usuarios con privilegios en el sistema.

Cada prueba tiene que ser realizada en la fecha planificada, por expertos con conocimientos suficientes del entorno a probar, o por especialistas externos contratados. Las pruebas planificadas y no realizadas en fecha tienen que ser consideradas con resultado insatisfactorio en el computo total.

Tiene que realizarse un informe de cada prueba, que debe ser distribuido, al Coordinador de Seguridad y al Director de Sistemas de Información, y guardado como documento auditable.

El computo para la obtención de los puntos correspondientes a este apartado se realiza obteniendo el porcentaje de las pruebas que han resultado satisfactorias frente al total de las realizadas.

7.3 B INVENTARIO Y CLASIFICACIÓN DE ACTIVOS

Deben ser planificadas anualmente actividades relacionadas con las aplicaciones y los Activos de Información procesados por ellas.

La revisión debe incluir:

el inventario de las aplicaciones de cada Función y de sus Activos de información;

la clasificación de todos los Activos de Información de cada una de las aplicaciones;

la renovación de Aplicaciones y Activos de Información críticos de las aplicaciones.

Debe ser realizada por los propietarios de aplicaciones, con la colaboración del coordinador funcional de Seguridad.

Como consecuencia de esta revisión, debe emitirse un informe al Director funcional, incluyendo las modificaciones realizadas y el resultado global de la actividad.

El coordinador funcional debe guardar el inventario de la Función y el informe de la revisión como documentos auditables. El computo para la obtención de los puntos correspondientes a este apartado se realiza obteniendo el porcentaje de las aplicaciones y los Activos revisados y actualizados frente al total de los existentes.

7.4 DIAGNÓSTICOS DE SEGURIDAD

Deben planificarse anualmente actividades para verificar que el nivel de implantación es el correcto y tener la posibilidad de detectar cualquier desviación de las normas y posibles deficiencias o

carencias. La planificación debe incluir una fecha de realización, que de no cumplirse equivaldría a un diagnóstico con resultados insatisfactorios.

Por el alcance y las características del equipo revisor, pueden dividirse en:

Autoevaluación, cuando una revisión es realizada por un equipo que pertenece a la propia Función.

Revisión, cuando el equipo es ajeno a la Función revisada y se cumple el principio de segregación de responsabilidades, pudiendo ser incluso externo a la empresa.

La revisión, en un sentido estricto, debe verificar el cumplimiento de lo establecido en las Normas y Procedimientos de Seguridad de la empresa y asesorar sobre las posibles deficiencias de protección.

Las desviaciones observadas y las deficiencias detectadas serán trasladadas a un informe para la Dirección, junto con las correspondientes recomendaciones para su corrección.

Auditoría, cuando el equipo revisor pertenece al departamento de auditoría de la empresa o se contrata a un grupo de expertos ajenos a la empresa. La auditoría, en un sentido estricto, debe verificar el cumplimiento de lo establecido en las Normas y Procedimientos de Seguridad de la empresa. Las desviaciones observadas serán trasladadas a un informe para la Dirección, junto con las correspondientes recomendaciones para subsanarlas.

Dependiendo del ámbito, una revisión o auditoría puede ser:

Funcional, cuando afectan sólo a una Función de la empresa.

Total, cuando la afectada es toda la empresa, incluyendo la función de Sistemas de Información.

Los requerimientos mínimos para la planificación deben ser:

Una autoevaluación por Función cada año.

Una revisión funcional por Función cada dos años, excepto en Sistemas de Información que debe ser anual.

Una revisión total de la empresa cada tres años.

Una auditoría total de la empresa cada tres años.

Esta periodicidad está basada en la obtención de resultados satisfactorios. Un resultado insatisfactorio en cualquiera de ellas obligaría a su repetición antes de 6 meses desde la fecha del informe.

La revisión o auditoría total de la empresa y la revisión funcional de Sistemas de Información tienen que incluir pruebas de integridad de sistemas, descritas en el apartado anterior.

Es importante la valoración individual de cada uno de los hechos que producen durante una revisión o auditoría. La siguiente tabla puede servir de orientación para la evaluación. Los criterios para valorar un hecho se basan en la clasificación de la información afectada y si existe, o no, una norma de Seguridad y su nivel de implantación.

Tabla 4. Evaluaciones en Diagnósticos de Seguridad Informática

INFORMACIÓN AFECTADA	NORMA IMPLANTADA	NORMA PARCIALMENTE IMPLANTADA	NORMA NO IMPLANTADA
PÚBLICA	POSIBLE COMENTARIO	IMPLANTACIÓN MEJORABLE	RIESGO MENOR
INTERNA	RIESGO MENOR	RIESGO POTENCIAL	RIESGO SIGNIFICATIVO
CONFIDENCIAL	RIESGO POTENCIAL	RIESGO SIGNIFICATIVO	RIESGO GRAVE
SECRETA	RIESGO SIGNIFICATIVO	RIESGO GRAVE	RIESGO GRAVE

NOTA: Si la información afectada, independientemente de la clasificación, pertenece a, o es necesaria para, un proceso esencial del negocio de la empresa, la valoración del hecho variará a un nivel superior de riesgo.

La evaluación final estará siempre en consonancia con la valoración individual de los hechos y tendrá el valor más alto de los encontrados, de acuerdo con la tabla siguiente.

Tabla 5. Evaluación Final del Diagnóstico de Seguridad Informática

RIESGOS ENCONTRADOS	VALORACIÓN FINAL	VALOR
COMENTARIO	Pleno Cumplimiento	1
MEJORABLE o RIESGO MENOR	Controlado	2
RIESGO POTENCIAL	Bajo Riesgo	3
RIESGO SIGNIFICATIVO	Riesgo Medio	4
RIESGO GRAVE	Alto Riesgo	5

NOTA: La acumulación de hechos en el más alto nivel de los encontrados, variará la valoración final a un nivel de menor cumplimiento.

Al término de cada revisión o auditoría debe crearse un informe de resultados que será presentado al más alto nivel de Dirección afectado y una copia enviada al Director de Seguridad.

Las desviaciones o deficiencias detectadas deben generar un Plan de Acción, encaminado a su corrección, incluyendo responsable de la actividad y fecha de terminación. Este plan tiene que ser realizado antes de 30 días, a contar desde la fecha del informe, para los resultados con valor final 3, 4 y 5. El Plan de Acción, su seguimiento y la implantación de las actividades incluidas en él, están sujetos a revisión o auditoría.

El computo para la obtención de los puntos correspondientes a este apartado se realiza obteniendo el porcentaje de las revisiones y auditorías con resultado satisfactorio (1 y 2) frente al total de las realizadas.

7.5 RECUPERACIÓN DE DESASTRES

Deben planificarse anualmente actividades a realizar para la recuperación de las aplicaciones críticas, los procesos vitales y los servicios esenciales de la empresa.

La planificación debe incluir un responsable de su realización y una fecha de terminación, que de no cumplirse convertiría la actividad en no realizada, para el computo de puntos obtenidos.

La planificación tiene que incluir la revisión y actualización de todos y cada uno de los procedimientos, y el plan de pruebas de recuperación a todos los niveles.

Entre las actividades planificadas tienen que incluirse:

- la revisión y actualización de procedimientos;
- la obtención periódica y en fecha de las copias de respaldo;
- las pruebas de continuidad de operaciones en el propio centro; o las pruebas de continuidad de operaciones en un centro alternativo;
- el plan de recuperación física del centro siniestrado;
- la vuelta al centro origen.

Las pruebas se consideran terminadas de forma satisfactoria, cuando se han podido recuperar el sistema y la información al mismo nivel que tenían en el momento de la declaración (presunta) del desastre.

El computo para la obtención de los puntos correspondientes a este apartado se realiza obteniendo el porcentaje de las actividades terminadas satisfactoriamente, y en fecha, frente al total de las planificadas.

7.6 OTRAS ACTIVIDADES DE SEGURIDAD

Deben planificarse anualmente otras actividades a realizar para la mejora o al menos el mantenimiento del nivel de Seguridad adquirido. En este apartado deben definirse las no incluidas en los anteriores

La planificación debe incluir un responsable de su realización y una fecha determinación, que de no cumplirse convertiría la actividad en no realizada, para el computo de puntos obtenidos.

Ejemplos de áreas de Seguridad a incluir en este apartado serían:

- protección física de Recursos Informáticos;
- gestión de Medios de Almacenamiento;
- protección de salidas impresas clasificadas;
- revisión y actualización de procedimientos;
- conexiones externas, etc.

ANEXO 1. EXTRACTO DE NORMATIVA LEGAL REFERENCIADA

LORTAD

ARTICULO 9. Seguridad de los Datos

El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Reglamentariamente se establecerá los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

ARTICULO 27(.2). Prestación de Servicios de Tratamiento Automatizado de Datos de Carácter Personal

2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que.medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma.la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años.

ARTICULO 43(.3h) Tipos de Infracciones.

3-Son infracciones graves:

h) Mantener los ficheros locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen.

LEY DE FACTURACIÓN TELEMÁTICA ARTICULO 4(.2f)

ARTICULO 4(.2f)

4. Procedimiento de autorización de la implantación o modificación de un sistema de intercambio de facturación por medios telemáticos.

Dos. Documentación a aportar.- Deberá adjuntarse al escrito de solicitud una memoria detallada con el.siguiente contenido mínimo:

f) Descripción de las medidas de seguridad incorporadas en los centros servidores, así como de las fórmulas o mecanismos que aseguran la integridad y exactitud de la información transmitida

ARTICULO 5(.2D)

5. Procedimiento de autorización a usuarios de un sistema de intercambio de facturación por medios telemáticos.

Dos.- Resolución de las solicitudes de autorización de usuarios de un sistema de intercambio de facturación por medios telemáticos. El Director del Departamento deInspección Financiera y Tributaria resolverá sobre las solicitudes de autorización recibidas, en el plazo de un mes desde su recepción, sin perjuicio del requerimiento al usuario de cuantos datos o nuevas informaciones resulten necesarias para la resolución del expediente de autorización, en cuyo caso se interrumpirá dicho plazo. Transcurridos los plazos señalados anteriormente sin mediar resolución expresa del Director del Departamento de Inspección Financiera y Tributaria se entenderá concedida la autorización.

Las relaciones de usuarios autorizados se comunicarán al promotor, que las pondrá en conocimiento de los centros servidores, al objeto de que procedan a la conservación de los datos de control conforme a lo dispuesto en esta Orden.

Las resoluciones dictadas por el Director del Departamento de Inspección Financiera y Tributaria serán reclamables en vía económico-administrativa, previo el recurso de reposición, si el interesado decidiera interponerlo.

Será causa de denegación de la autorización el incumplimiento de cualquiera de las disposiciones establecidas en el Real Decreto 2402/85, de 18 de diciembre, de esta Orden, y en las Resoluciones de la Agencia Estatal de Administración Tributaria que la desarrollen, y en particular: d) La falta de procedimientos y controles que aseguren la conservación del contenido original y, en el orden cronológico, de la información que ..está obligado a tener a disposición de la Administración Tributaria durante el período de prescripción. Así como la .inexistencia de programas y ficheros de datos necesarios que permitan la reconstrucción completa del camino de auditoría del usuario.

ARTICULO 6(.1)

6. Obligaciones del promotor de un sistema de intercambio de facturación por medios telemáticos.

Uno. Obligaciones.- El promotor es responsable de la adopción de los controles suficientes para asegurar el cumplimiento de.las condiciones y requisitos establecidos en esta Orden, en las resoluciones de la Agencia Estatal de Administración Tributaria que se dicten en desarrollo de la misma, así como en el expediente de autorización y, asimismo, estará obligado a:

a) Facilitar a la Inspección de los Tributos el acceso a sus instalaciones y a proporcionar todo tipo de datos, antecedentes y justificantes, incluidos los registrados en soportes electrónicos, y permitan la obtención de copias y la realización de las pruebas necesarias para verificar si el sistema ajusta sus especificaciones a los requerimientos administrativos. Asimismo, deberá facilitar los documentos y pruebas de auditoría informática que, en su caso, se realicen sobre el sistema por auditores externos.

b) Conservar, durante el período de prescripción del derecho de la Administración para determinar las deudas tributarias afectadas por las operaciones correspondientes, un fichero histórico de los usuarios del sistema de intercambio de facturación por medios telemáticos gestionado con indicación de su fecha de alta y baja, en su caso, así como razón social, número de identificación fiscal y código interno de usuario. Copia de este fichero será presentada ante el Departamento de Inspección Financiera y Tributaria con carácter anual durante el mes de enero de cada año.

c) Disponer, en los centros servidores, de los debidos procedimientos y controles que aseguren la conservación de contenido original, en orden cronológico, de la información que está obligando a tener a disposición de Administración Tributaria durante el período de prescripción.

d) Conservar durante el mismo período un diario por el método de partida doble de la actividad de cada centro servidor, en el que figuren debidamente saldadas, a nivel de cada transmisión, las facturas recibidas con las imputaciones realizadas en la recepción, y las facturas transmitidas con sus respectivos orígenes en la emisión de cada centro servidor. Los asientos incorporarán como referencia obligatoria un número interno y seriado de operación. El contenido del diario mencionado en el párrafo anterior se conservará en soporte magnético u óptico, con las características que se desarrollen en el anexo II de la presente Orden.

e) En los supuestos de intercambio de facturas electrónicas con mediación de más de un centro servidor, será obligatoria la información relativa al código de centro servidor interlocutor de origen o destino de la información en el diario antes mencionado.

f) El promotor deberá conservar separadamente, durante el período de prescripción, el diario histórico de los mensajes de iniciativas que se produzcan, que contendrá información suficiente que permita identificar a los usuarios afectados, día y hora de la transmisión e identificación de la incidencia ocurrida, así como del documento en el que se originó. En los casos de incidencias o anomalías en la transmisión, se realizarán los asientos de ajustes que procedan conforme al diario histórico de mensajes de incidencia.

g) Notificar a los usuarios del sistema todas las modificaciones debidamente autorizadas, así como los supuestos de suspensión o caducidad.

h) Comunicar al Director del Departamento de Inspección Financiera y Tributaria los casos de cese y cualquier cambio en la titularidad de la actividad del promotor. Dicho escrito deberá presentarse en el plazo máximo de los treinta días naturales siguientes a la fecha de cese.

ARTÍCULO 7(.b)

> **7.** Obligaciones del usuario de un sistema de intercambio de facturación por medios telemáticos.
>
> Cualquier usuario autorizado a operar en un sistema de intercambio.de facturación por medios telemáticos estará obligado a:

b) Adoptar las medidas de seguridad necesarias tales como doble copia, regrabación periódica, o cualquier otra que, técnicamente, permita garantizar la lectura y recuperación de los datos que debe conservar durante el período de prescripción al objeto de facilitar su visualización en pantalla, su impresión en soporte papel o copia en soporte magnético a petición de la inspección de los Tributos.

LEY DE ORDENACIÓN DE LAS TELECOMUNICACIONES

> **ARTICULO 5(.4)**

5. Los centros, establecimientos y dependencias afectos a los servicios de telecomunicación, dispondrán de las medidas y sistemas de seguridad, vigilancia, difusión de información, prevención de riesgos y protección que se determinen por el Gobierno, a propuesta de los Ministerios de Defensa, Interior o Transporte, Turismo y Comunicaciones, dentro del ámbito de sus respectivas competencias, tanto en situaciones de normalidad o de crisis como en los supuestos contemplados por la Ley de Protección Civil, por la Ley Orgánica reguladora.de los estados de alarma, excepción y sitio o en tiempos de guerra.

ARTICULO 24

1. En todo caso, las entidades que explotan los servicios de valor añadido estarán obligadas a cumplir las especificaciones de los puntos de terminación de los servicios finales y portadores de telecomunicación que utilicen. A tal fin, los equipos que conecten a dichos puntos de terminación de la red tendrán necesariamente que haber obtenido los correspondientes certificados de homologación y de aceptación de las citadas especificaciones para garantizar tanto la seguridad del usuario como el correcto funcionamiento de la red de telecomunicación.

2. Las entidades que presten a terceros servicios de valor añadido en régimen de concesión deberán presentar a la Administración cuentas anuales en las que se especifique la participación de cada uno de dichos servicios en sus ingresos o costes.

3. El Ministerio de Obras Públicas y Transportes establecerá un Registro Central de Servicios de Valor Añadido otorgados en régimen de concesión en el que deberán estar inscritos todos los datos que reglamentariamente se determinen, tanto respecto al explotador del servicio como a las condiciones y características del mismo.

4. Las entidades explotadoras de servicios de valor añadido vendrán obligadas a garantizar el secreto de las comunicaciones en el marco de lo dispuesto en el artículo dos, apartado segundo, de la presente Ley, y aplicar el principio de no discriminación, en el acceso al servicio, de ningún potencial usuario del mismo, siempre que se encuentre dentro de la zona de cobertura del mismo y se disponga de instalaciones suficientes para ello, todo esto sin perjuicio de lo que establece en la Ley General para la Defensa de los Consumidores y Usuarios.

REAL DECRETO

1382/85 RD 1382/85 de 1 de agosto, por el que se regula la relación laboral de carácter especial del personal de alta dirección. ("B.O.E." núm. 192 de 12-VIII-1995).

El artículo segundo, uno,

a) del Estatuto de los Trabajadores.considera relación laboral de carácter especial a la del personal de alta dirección no incluido en el artículo primero,.tres,

c) de la propia norma, estableciéndose en la disposición adicional a la primera de la Ley 32/1984, de 2 de agosto, sobre modificación de determinados artículos del Estatuto de los Trabajadores, como el Gobierno, en el plazo máximo de doce meses contados a partir de la entrada en vigor de la referenciada Ley, habría que regular el régimen jurídico en el Estatuto de los Trabajadores.

Mediante la presente norma se da cumplimiento a tal mandato, teniéndose en cuenta fundamentalmente para fijar su contenido el que la relación establecida entre el alto directivo y la Empresa contratante se caracteriza por la recíproca confianza que debe existir entre ambas partes, derivada de la singular posición que el directivo asume en el ámbito de la Empresa en cuanto a facultades y poderes. Estas características se reflejan en el

régimen jurídico que .establece la presente norma, que en primer lugar determina .el concepto del personal de alta dirección, para delimitar el ámbito de la norma, eliminándose así situaciones de indefinición jurídica, e incluso vacío de regulación, que se había venido produciendo por esta falta de tratamiento normativo.
Precisamente por estas características de la relación que une al directivo con le Empresa se ha optado por proporcionar un amplio margen al pacto entre las partes de esta relación, como elemento de configuración del contenido de la misma, correspondiendo a la norma por su parte el fijar el esquema básico de la materia a tratar en el contrato, profundizado más en cuestiones como, por ejemplo, las relativas a las causas y efectos de extinción de contrato, respecto de las que se ha considerado debía existir un tratamiento normativo más completo, al ser menos susceptibles de acuerdos entre partes.
En su virtud, consultadas las Organizaciones Sindicales y Patronales más representativas, de acuerdo con el Consejo de Estado, a propuesta del Ministerio de Trabajo y Seguridad Social, y previa deliberación del Consejo de Ministros en su reunión del día 31 de julio de 1985.

DISPONGO:

ARTICULO 1. Ámbito de Aplicación.

Uno. El presente Real Decreto, de acuerdo con el artículo 2.1.a) de la Ley 8/1980, de 10 de marzo, del Estatuto de los Trabajadores, y al amparo de la disposición adicional primera de la Ley 32/1984, de 2 de agosto, regula la relación laboral de carácter especial del personal de alta dirección.

Dos. Se considera personal de alta dirección a aquellos trabajadores que ejercitan poderes inherentes a la titularidad jurídica de la Empresa, y relativos a los objetivos generales de la misma, con autonomía y plena responsabilidad sólo limitadas por los criterios e instrucciones directas emanadas de la persona o de los órganos superiores de gobierno y administración de la Entidad que respectivamente ocupe aquella titularidad.

Tres. Se excluye del ámbito de este Real Decreto la actividad delimitada en el artículo 1.3.c) del Estatuto de los Trabajadores.

ARTICULO 2

Fundamento. La relación laboral especial del personal de alta dirección se basa en la recíproca confianza de las partes, las cuales acomodarán el ejercicio de sus derechos y obligaciones a las exigencias de la buena fe.

ARTICULO 3

Fuentes y Criterios Reguladores.

Uno. Los derechos y obligaciones concernientes a la relación laboral del personal de alta dirección se regularán por la voluntad de las partes, con sujeción a las normas de este Real Decreto y a las demás que sean de aplicación.

Dos. Las demás normas de la legislación laboral común, incluido el Estatuto de los Trabajadores, sólo serán aplicables en los casos en que se produzcan remisión expresa en este Real Decreto, o así se haga constar específicamente en el contrato.

Tres. En lo no regulado por este Real Decreto o por pacto entre las partes, se estará a lo dispuesto en la legislación civil o mercantil y a sus principios generales.

NUEVO CÓDIGO PENAL

ARTICULO 197

1 El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2 Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3 Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Serán castigados con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, los que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizaren la conducta descrita en el párrafo anterior.

4 Si los hechos descritos en los párrafos 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena de su mitad superior.

5 Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere menor de edad o incapaz, se impondrán las penas previstas en su mitad superior.

6 Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a seis años.

ARTICULO 256

El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

ARTICULO 264 (.2)

2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

ARTICULO 278

1- El que, para descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado por la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3- Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos

ARTICULO 400

La fabricación o tenencia de útiles, materiales, instrumentos, sustancias,máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.