INSTITUTO ARGENTINO DE NORMALIZACIÓN

ESQUEMA 1

DE NORMA IRAM-ISO IEC 17799

Tecnología de la información

Código de práctica para la administración de la seguridad de la información

Information technology.
Code of practice for information security management.

Este esquema está sometido a discusión pública. Las observaciones deben remitirse fundadas y por escrito, al Instituto IRAM, Perú 552 / 556 - (C1068AAB) Buenos Aires antes del 2002-06-28

DOCUMENTO EN ESTUDIO

xxxx de 2002

Prefacio

El Instituto Argentino de Normalización (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

Esta norma es una adopción idéntica de la norma ISO 17799:2000.

Índice

Página

INTRODUCCIÓN 6

QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN ? 6
POR QUÉ ES NECESARIA LA SEGURIDAD DE LA INFORMACIÓN 6
CÓMO ESTABLECER LOS REQUERIMIENTOS DE SEGURIDAD 6
EVALUACIÓN DE LOS RIESGOS EN MATERIA DE SEGURIDAD 6
SELECCIÓN DE CONTROLES 6
PUNTO DE PARTIDA PARA LA SEGURIDAD DE LA INFORMACIÓN 6
FACTORES CRÍTICOS DEL ÉXITO 6
DESARROLLO DE LINEAMIENTOS PROPIOS 6

1 ALCANCE 6

2 TÉRMINOS Y DEFINICIONES 6

3 POLÍTICA DE SEGURIDAD 6

3.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 6
3.1.1 Documentación de la política de seguridad de la información 6
3.1.2 Revisión y evaluación 6

4 ORGANIZACIÓN DE LA SEGURIDAD 6

4.1 INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN 6
4.1.1 Foro gerencial sobre seguridad de la información 6
4.1.2 Coordinación de la seguridad de la información 6
4.1.3 Asignación de responsabilidades en materia de seguridad de la información 6
4.1.4 Proceso de autorización para instalaciones de procesamiento de información 6
4.1.5 Asesoramiento especializado en materia de seguridad de la información 6
4.1.6 Cooperación entre organizaciones 6
4.1.7 Revisión independiente de la seguridad de la información 6
4.2 SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS 6
4.2.1 Identificación de riesgos del acceso de terceras partes 6
4.2.2 Requerimientos de seguridad en contratos con terceros 6
4.3 TERCERIZACIÓN 6
4.3.1 Requerimientos de seguridad en contratos de tercerización 6

5 CLASIFICACIÓN Y CONTROL DE ACTIVOS 6

5.1 RESPONSABILIDAD POR RENDICIÓN DE CUENTAS DE LOS ACTIVOS 6
5.1.1 Inventario de activos 6
5.2 CLASIFICACIÓN DE LA INFORMACIÓN 6
5.2.1 Pautas de clasificación 6
5.2.2 Rotulado y manejo de la información 6

6 SEGURIDAD DEL PERSONAL 6

6.1 SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS 6
6.1.1 Inclusión de la seguridad en las responsabilidades de los puestos de trabajo 6

6.1.2 Selección y política de personal ... *6*
6.1.3 Acuerdos de confidencialidad ... *6*
6.1.4 Términos y condiciones de empleo ... *6*
6.2 CAPACITACIÓN DEL USUARIO ... 6
6.2.1 Formación y capacitación en materia de seguridad de la información ... *6*
6.3 RESPUESTA A INCIDENTES Y ANOMALÍAS EN MATERIA DE SEGURIDAD ... 6
6.3.1 Comunicación de incidentes relativos a la seguridad ... *6*
6.3.2 Comunicación de debilidades en materia de seguridad ... *6*
6.3.3 Comunicación de anomalías del software ... *6*
6.3.4 Aprendiendo de los incidentes ... *6*
6.3.5 Proceso disciplinario ... *6*

7 SEGURIDAD FÍSICA Y AMBIENTAL ... 6

7.1 ÁREAS SEGURAS ... 6
7.1.1 Perímetro de seguridad física ... *6*
7.1.2 Controles de acceso físico ... *6*
7.1.3 Protección de oficinas, recintos e instalaciones ... *6*
7.1.4 Desarrollo de tareas en áreas protegidas ... *6*
7.1.5 Aislamiento de las áreas de entrega y carga ... *6*
7.2 SEGURIDAD DEL EQUIPAMIENTO ... 6
7.2.1 Ubicación y protección del equipamiento ... *6*
7.2.2 Suministros de energía ... *6*
7.2.3 Seguridad del cableado ... *6*
7.2.4 Mantenimiento de equipos ... *6*
7.2.5 Seguridad del equipamiento fuera del ámbito de la organización ... *6*
7.2.6 Baja segura o reutilización de equipamiento. ... *6*
7.3 CONTROLES GENERALES ... 6
7.3.1 Políticas de escritorios y pantallas limpias. ... *6*
7.3.2 Retiro de bienes ... *6*

8 GESTIÓN DE COMUNICACIONES Y OPERACIONES ... 6

8.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS ... 6
8.1.1 Documentación de los procedimientos operativos ... *6*
8.1.2 Control de cambios en las operaciones ... *6*
8.1.3 Procedimientos de manejo de incidentes ... *6*
8.1.4 Separación de funciones ... *6*
8.1.5 Separación entre instalaciones de desarrollo e instalaciones operativas ... *6*
8.1.6 Administración de instalaciones externas ... *6*
8.2 PLANIFICACIÓN Y APROBACIÓN DE SISTEMAS ... 6
8.2.1 Planificación de la capacidad ... *6*
8.2.2 Aprobación del sistema ... *6*
8.3 PROTECCIÓN CONTRA SOFTWARE MALICIOSO ... 6
8.3.1 Controles contra software malicioso ... *6*
8.4 MANTENIMIENTO ... 6
8.4.1 Resguardo de la información ... *6*
8.4.2 Registro de actividades del personal operativo ... *6*
8.4.3 Registro de fallas ... *6*
8.5 ADMINISTRACIÓN DE LA RED ... 6
8.5.1 Controles de redes ... *6*
8.6 ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO ... 6
8.6.1 Administración de medios informáticos removibles ... *6*
8.6.2 Eliminación de medios informáticos ... *6*
8.6.3 Procedimientos de manejo de la información ... *6*
8.6.4 Seguridad de la documentación del sistema ... *6*
8.7 INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE ... 6
8.7.1 Acuerdos de intercambio de información y software ... *6*
8.7.2 Seguridad de los medios en tránsito ... *6*

8.7.3 Seguridad del comercio electrónico 6
8.7.4 Seguridad del correo electrónico 6
8.7.5 Seguridad de los sistemas electrónicos de oficina 6
8.7.6 Sistemas de acceso público 6
8.7.7 Otras formas de intercambio de información 6

9 CONTROL DE ACCESOS 6

9.1 REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESOS 6
9.1.1 Política de control de accesos 6
9.2 ADMINISTRACIÓN DE ACCESOS DE USUARIOS 6
9.2.1 Registración de usuarios 6
9.2.2 Administración de privilegios 6
9.2.3 Administración de contraseñas de usuario 6
9.2.4 Revisión de derechos de acceso de usuario 6
9.3 RESPONSABILIDADES DEL USUARIO 6
9.3.1 Uso de contraseñas 6
9.3.2 Equipos desatendidos en áreas de usuarios 6
9.4 CONTROL DE ACCESO A LA RED 6
9.4.1 Política de utilización de los servicios de red 6
9.4.2 Camino forzado 6
9.4.3 Autenticación de usuarios para conexiones externas 6
9.4.4 Autenticación de nodos 6
9.4.5 Protección de los puertos (ports) de diagnostico remoto 6
9.4.6 Subdivisión de redes 6
9.4.7 Control de conexión a la red 6
9.4.8 Control de ruteo de red 6
9.4.9 Seguridad de los servicios de red 6
9.5 CONTROL DE ACCESO AL SISTEMA OPERATIVO 6
9.5.1 Identificación automática de terminales 6
9.5.2 Procedimientos de conexión de terminales 6
9.5.3 Identificación y autenticación de los usuarios 6
9.5.4 Sistema de administración de contraseñas 6
9.5.5 Uso de utilitarios de sistema 6
9.5.6 Alarmas silenciosas para la protección de los usuarios 6
9.5.7 Desconexión de terminales por tiempo muerto 6
9.5.8 Limitación del horario de conexión 6
9.6 CONTROL DE ACCESO A LAS APLICACIONES 6
9.6.1 Restricción del acceso a la información 6
9.6.2 Aislamiento de sistemas sensibles 6
9.7 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS 6
9.7.1 Registro de eventos 6
9.7.2 Monitoreo del uso de los sistemas 6
9.7.3 Sincronización de relojes 6
9.8 COMPUTACIÓN MÓVIL Y TRABAJO REMOTO 6
9.8.1 Computación móvil 6
9.8.2 Trabajo remoto 6

10 DESARROLLO Y MANTENIMIENTO DE SISTEMAS. 6

10.1 REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS. 6
10.1.1 Análisis y especificaciones de los requerimientos de seguridad. 6
10.2 SEGURIDAD EN LOS SISTEMAS DE APLICACIÓN 6
10.2.1 Validación de datos de entrada 6
10.2.2 Controles de procesamiento interno. 6
10.2.3 Autenticación de mensajes 6
10.2.4 Validación de los datos de salida 6
10.3 CONTROLES CRIPTOGRÁFICOS 6
10.3.1 Política de utilización de controles criptográficos 6
10.3.2 Cifrado 6

10.3.3 Firma digital *6*
10.3.4 Servicios de no repudio *6*
10.3.5 Administración de claves *6*
10.4 SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA 6
10.4.1 Control del software operativo *6*
10.4.2 Protección de los datos de prueba del sistema *6*
10.4.3 Control de acceso a las bibliotecas de programa fuente *6*
10.5 SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE 6
10.5.1 Procedimientos de control de cambios *6*
10.5.2 Revisión técnica de los cambios en el sistema operativo *6*
10.5.3 Restricción del cambio en los paquetes de software *6*
10.5.4 Canales ocultos y código troyano *6*
10.5.5 Desarrollo externo de software *6*

11 ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS 6

11.1 ASPECTOS DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS 6
11.1.1 Proceso de administración de la continuidad de los negocios *6*
11.1.2 Continuidad del negocio y análisis del impacto *6*
11.1.3 Elaboración e implementación de planes de continuidad de los negocios *6*
11.1.4 Marco para la planificación de la continuidad de los negocios *6*
11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios *6*

12 CUMPLIMIENTO 6

12.1 CUMPLIMIENTO DE REQUISITOS LEGALES 6
12.1.1 Identificación de la legislación aplicable *6*
12.1.2 Derechos de propiedad intelectual (dpi) *6*
12.1.3 Protección de los registros de la organización *6*
12.1.4 Protección de datos y privacidad de la información personal *6*
12.1.5 Prevención del uso inadecuado de los recursos de procesamiento de información *6*
12.1.6 Regulación de controles para el uso de criptografía *6*
12.1.7 Recolección de evidencia *6*
12.2 REVISIONES DE LA POLÍTICA DE SEGURIDAD Y LA COMPATIBILIDAD TÉCNICA 6
12.2.1 Cumplimiento de la política de seguridad *6*
12.2.2 Verificación de la compatibilidad técnica *6*
12.3 CONSIDERACIONES DE AUDITORIA DE SISTEMAS 6
12.3.1 Controles de auditoria de sistemas *6*
12.3.2 Protección de las herramientas de auditoría de sistemas *6*

Anexo A (Informativo) Bibliografía 6

Anexo B (Informativo) Integrantes del organismo de estudio 6

Tecnología de la información

Código de práctica para la administración de la seguridad de la información

INTRODUCCIÓN

Qué es la seguridad de la información ?

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

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

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

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

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software.

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

Por qué es necesaria la seguridad de la información

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

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

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

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

Cómo establecer los requerimientos de seguridad

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

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

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

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

Evaluación de los riesgos en materia de seguridad

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

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

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

Los resultados de esta evaluación ayudarán a orientar ya determinar las prioridades y acciones de gestión adecuadas para la administración de los riesgos concernientes a seguridad de la información, y para la implementación de los controles seleccionados a fin de brindar protección contra dichos riesgos.

Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

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

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

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

Selección de controles

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. Los controles pueden seleccionarse sobre la base de este documento, de otros estándares, o pueden diseñarse nuevos controles para satisfacer necesidades específicas según corresponda. Existen diversos modos de administrar riesgos y este documento brinda ejemplos de estrategias generales. No obstante, es necesario reconocer que algunos controles no son aplicables a todos los sistemas o ambientes de información, y podrían no resultar viables en todas las organizaciones. Como ejemplo, el punto 8.1.4 describe cómo pueden separarse las tareas para evitar fraudes y errores. Podría no resultar posible para las organizaciones más pequeñas separar todas las tareas, pudiendo resultar necesarias otras formas de lograr el mismo objetivo de control.

Los controles deben seleccionarse teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño en la reputación.

Algunos controles de este documento pueden considerarse como principios rectores para la administración de la seguridad de la información, aplicables a la mayoría de las organizaciones. Se explican con mayor detalle en el siguiente párrafo, bajo el título de "Punto de partida para la seguridad de la información".

Punto de partida para la seguridad de la información

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

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

a) protección de datos y confidencialidad de la información personal (ver 12.1.4);
b) protección de registros y documentos de la organización (ver 12.1.3) ;
c) derechos de propiedad intelectual (ver 12.1.2) ;

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

a) documentación de la política de seguridad de la información (ver 3.1.1);
b) asignación de responsabilidades en materia de seguridad de la información (ver 4.1 .3);
c) instrucción y entrenamiento en materia de seguridad de la información (ver 6.2.1);
d) comunicación de incidentes relativos a la seguridad (ver 6.3.1);
e) administración de la continuidad de la empresa (ver 11.1);

Estos controles son aplicables a la mayoría de las organizaciones y en la mayoría de los ambientes.

Se debe observar que aunque todos los controles mencionados en este documento son importantes, la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que afronta la organización. Por ello, si bien el enfoque delineado precedentemente se considera un buen punto de partida, éste no pretende reemplazar la selección de controles que se realiza sobre la base de una evaluación de riesgos.

Factores críticos del éxito

La experiencia ha demostrado que los siguientes factores, a menudo resultan críticos para la implementación exitosa de la seguridad de la información, dentro de una organización:

a) política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa;
b) una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional;
c) apoyo y compromiso manifiestos por parte de la gerencia;
d) un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos;
e) comunicación eficaz de los temas de seguridad a todos los gerentes y empleados;
f) distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas;
g) instrucción y entrenamiento adecuados;
h) un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

Desarrollo de lineamientos propios

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

1 ALCANCE

Esta parte del estándar brinda recomendaciones para la gestión de la seguridad de la información que han de ser aplicadas por los responsables de iniciar, implementar o mantener la seguridad en sus organizaciones. Su propósito es proveer de una base común para el desarrollo de estándares de seguridad de la organización y una práctica efectiva de la administración de la misma, brindando asimismo, confianza en las relaciones llevadas a cabo entre las organizaciones.

2 TÉRMINOS Y DEFINICIONES

A los efectos de este documento se aplican las siguientes definiciones:

2.1 Seguridad de la información

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

- Confidencialidad: garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo.
- Integridad: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

2.2 Evaluación de riesgos

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

2.3 Administración de riesgos

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

3 POLÍTICA DE SEGURIDAD

3.1 Política de seguridad de la información

Objetivo: Proporcionar dirección y apoyo gerencial para brindar seguridad de la información. El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

3.1.1 Documentación de la política de seguridad de la información

Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información. Como mínimo, deben incluirse las siguientes pautas:

a) definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información (ver introducción);
b) una declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información;
c) una breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la organización, por ejemplo:
    1) cumplimiento de requisitos legales y contractuales;
    2) requisitos de instrucción en materia de seguridad;
    3) prevención y detección de virus y demás software malicioso;
    4) administración de la continuidad comercial;
    5) consecuencias de las violaciones a la política de seguridad;

d) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluyendo la comunicación de los incidentes relativos a la seguridad;
e) referencias a documentos que puedan respaldar la política, por ej. , políticas y procedimientos de seguridad más detallados para sistemas de información específicos o normas de seguridad que deben cumplir los usuarios.

Esta política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

3.1.2 Revisión y evaluación

La política debe tener un propietario que sea responsable del mantenimiento y revisión de la misma de acuerdo con un proceso definido. Ese proceso debe garantizar que se lleve acabo una revisión en respuesta a cualquier cambio que pueda afectar la base original de evaluación de riesgos, por ej., incidentes de seguridad significativos, nuevas vulnerabilidades o cambios en la infraestructura técnica o de la organización. También deben programarse revisiones periódicas de lo siguiente:

a) la eficacia de la política, demostrada por la naturaleza, número e impacto de los incidentes de seguridad registrados;
b) el costo e impacto de los controles en la eficiencia del negocio;
c) los efectos de los cambios en la tecnología.

4 ORGANIZACIÓN DE LA SEGURIDAD

4.1 Infraestructura de seguridad de la información

Objetivo: Administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

4.1.1 Foro gerencial sobre seguridad de la información

La seguridad de la información es una responsabilidad de la empresa compartida por todos los miembros del equipo gerencial. Por consiguiente, debe tenerse en cuenta la creación de un foro gerencial para garantizar que existe una clara dirección y un apoyo manifiesto de la gerencia a las iniciativas de seguridad. Este foro debe promover la seguridad dentro de la organización mediante un adecuado compromiso y una apropiada reasignación de recursos. El foro podría ser parte de un cuerpo gerencial existente. Generalmente, un foro de esta índole comprende las siguientes acciones:

a) revisar y aprobar la política y las responsabilidades generales en materia de seguridad de la información;
b) monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes;
c) revisar y monitorear los incidentes relativos a la seguridad;
d) aprobar las principales iniciativas para incrementar la seguridad de la información.

Un gerente debe ser responsable de todas las actividades relacionadas con la seguridad.

4.1.2 Coordinación de la seguridad de la información

En una gran organización, podría ser necesaria la creación de un foro ínter funcional que comprenda representantes gerenciales de sectores relevantes de la organización para coordinar la implementación de controles de seguridad de la información.

Normalmente, dicho foro:

a) acuerda funciones y responsabilidades específicas relativas a seguridad de la información para toda la organización;
b) acuerda metodologías y procesos específicos relativos a seguridad de la información, por ej., evaluación de riesgos, sistema de clasificación de seguridad;

c) acuerda y brinda apoyo a las iniciativas de seguridad de la información de toda la organización, por ej. programa de concientización en materia de seguridad;
d) garantiza que la seguridad sea parte del proceso de planificación de la información;
e) evalúa la pertinencia y coordina la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;
f) revisa incidentes relativos a la seguridad de la información;
g) promueve la difusión del apoyo de la empresa a la seguridad de la información dentro de la organización.

4.1.3 Asignación de responsabilidades en materia de seguridad de la información

Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad.
La política de seguridad de la información (ver punto 3) debe suministrar una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro la organización. Esto debe complementarse, cuando corresponda, con una guía más detallada para sitios, sistemas o servicios específicos. Deben definirse claramente las responsabilidades locales para cada uno de los procesos de seguridad y recursos físicos y de información, como la planificación de la continuidad de los negocios.

En muchas organizaciones, se asigna a un gerente de seguridad de la información la responsabilidad general por el desarrollo e implementación de la seguridad y por el soporte a la identificación de controles. No obstante, la responsabilidad por la reasignación e implementación de controles a menudo es retenida por cada uno de los gerentes. Una práctica común es designar a un propietario para cada recurso de información que además se haga responsable de su seguridad de manera permanente.
Los propietarios de los recursos de información pueden delegar sus responsabilidades de seguridad a cada uno de los gerentes o proveedores de servicios. No obstante, el propietario es en último término responsable de la seguridad del recurso y debe estar en capacidad de determinar si las responsabilidades delegadas fueron cumplimentadas correctamente.

Es esencial que se establezcan claramente las áreas sobre las cuales es responsable cada gerente; en particular se debe cumplir lo siguiente.

a) Deben identificarse y definirse claramente los diversos recursos y procesos de seguridad relacionados con cada uno de los sistemas.
b) Se debe designar al gerente responsable de cada recurso o proceso de seguridad y se deben documentar los detalles de esta responsabilidad.
c) Los niveles de autorización deben ser claramente definidos y documentados.

4.1.4 Proceso de autorización para instalaciones de procesamiento de información

Debe establecerse un proceso de autorización gerencial para nuevas instalaciones de procesamiento de información. Debe considerarse lo siguiente.

a) Las nuevas instalaciones deben ser adecuadamente aprobadas por la gerencia usuaria, autorizando su propósito y uso. La aprobación también debe obtenerse del gerente responsable del mantenimiento del ambiente de seguridad del sistema de información local, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.
b) Cuando corresponda, debe verificarse el hardware y software para garantizar que son compatibles con los componentes de otros sistemas.

Nota: Puede ser necesaria la comprobación de categorías para ciertas conexiones.

c) Deben ser autorizados el uso de las instalaciones personales de procesamiento de información, para el procesamiento de información de la empresa, y los controles necesarios.
d) El uso de instalaciones personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades y en consecuencia debe ser evaluado y autorizado.

Estos controles son especialmente importantes en un ambiente de red.

4.1.5 Asesoramiento especializado en materia de seguridad de la información

Es probable que muchas organizaciones requieran asesoramiento especializado en materia de seguridad. Idealmente, éste debe ser provisto por un asesor interno experimentado en seguridad de la información. No todas las organizaciones desean emplear aun asesor especializado. En esos casos, se recomienda que se identifique a una persona determinada para coordinar los conocimientos y experiencias disponibles en la organización a fin de garantizar coherencia, y brindar ayuda para la toma de decisiones en materia de seguridad. También debe tener acceso a calificados asesores externos para brindar asesoramiento especializado más allá de su propia experiencia.

Los asesores en seguridad de la información o puntos de contacto equivalentes serán los encargados de brindar asesoramiento acerca de todos los aspectos de la seguridad de la información, utilizando sus propias recomendaciones o las externas. La calidad de su evaluación de las amenazas a la seguridad y de su asesoramiento en materia de controles determinará la eficacia de la seguridad de la información de la organización. Para lograr la máxima eficacia e impacto se les debe permitir acceso directo a los niveles gerenciales de toda la organización.

El asesor de seguridad de la información o cargo equivalente debe ser consultado lo más tempranamente posible a partir de la detección de un supuesto incidente o violación de la seguridad, a fin de suministrar una fuente de conocimientos o recursos de investigación expertos. Si bien la mayoría de las investigaciones de seguridad internas se llevan a cabo bajo el control de la gerencia, el asesor de seguridad de la información puede ser posteriormente convocado para asesorar, liderar o dirigir la investigación.

4.1.6 Cooperación entre organizaciones

Se deben mantener adecuados contactos con autoridades policiales o de seguridad, organismos reguladores, proveedores de servicios de información y operadores de telecomunicaciones, a fin de garantizar que, en caso de producirse un incidente relativo a la seguridad, puedan tomarse las medidas adecuadas y obtenerse asesoramiento con prontitud. Del mismo modo, se debe tener en cuenta a los miembros de grupos de seguridad y foros de la industria.

Se deben limitar los intercambios de información de seguridad, para garantizar que no se divulgue información confidencial, perteneciente a organización, entre personas no autorizadas.

4.1.7 Revisión independiente de la seguridad de la información

El documento que fija la política de seguridad de la información (ver 3.1.1) establece la política y las responsabilidades por la seguridad de la información. Su implementación debe ser revisada independientemente para garantizar que las prácticas de la organización reflejan adecuadamente la política, y que ésta es viable y eficaz (ver 12.2.)

Dicha revisión puede ser llevada a cabo por la función de auditoría interna, por un gerente independiente o una organización externa especializados en revisiones de esta índole, según estos candidatos tengan la experiencia y capacidad adecuada.

4.2 Seguridad frente al acceso por parte de terceros

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.
Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control.
Los controles deben ser acordados y definidos en un contrato con la tercera parte.
El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso.
Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

4.2.1 Identificación de riesgos del acceso de terceras partes

4.2.1.1 Tipos de acceso

El tipo de acceso otorgado a terceras partes es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico. Los tipos de acceso que deben tenerse en cuenta son:

a) acceso físico, por ej., a oficinas, salas de cómputos, armarios ;
b) acceso lógico, por ej. a las bases de datos y sistemas de información de la organización.

4.2.1.2 Razones para el acceso

Puede otorgarse acceso a terceros por diversas razones. Por ejemplo, existen terceros que proveen servicios a una organización y no están ubicados dentro de la misma pero se les puede otorgar acceso físico y lógico, tales como:

a) personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones;
b) socios comerciales o socios con riesgos compartidos ("joint ventures"), quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

La información puede ponerse en riesgo si el acceso de terceros se produce en el marco de una inadecuada administración de la seguridad. Cuando existe una necesidad de negocios que involucran una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Ésta debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la organización.

4.2.1.3 Contratistas in situ

Las terceras partes que sean ubicadas in situ por un período de tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se enumeran los siguientes:

a) personal de mantenimiento y soporte de hardware y software;
b) limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados;
c) pasantías de estudiantes y otras designaciones contingentes de corto plazo;
d) consultores.

Es esencial determinar qué controles son necesarios para administrar el acceso de terceras partes a las instalaciones de procesamiento de información. En general, todos los requerimientos de seguridad que resultan de los controles internos o del acceso de terceros, deben estar reflejados en los contratos celebrados con los mismos (ver también 4.2.2). Por ejemplo, si existe una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación (ver 6.1.3).

No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.

4.2.2 Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización. El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor. Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

a) la política general de seguridad de la información;
b) la protección de activos, con inclusión de:
    1) procedimientos de protección de los activos de la organización, incluyendo información y software;
    2) procedimientos para determinar si se han comprometido los activos, por ej., debido a pérdida o modificación de datos;
    3) controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo;
    4) integridad y disponibilidad;
    5) restricciones a la copia y divulgación de información;
c) una descripción de cada servicio del que podrá disponerse;
d) el nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables;
e) disposición que contemple la transferencia de personal cuando corresponda;
f) las respectivas obligaciones de las partes con relación al acuerdo;
g) responsabilidades con respecto a asuntos legales, por ej., legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países (ver también 12.1);

h) derechos de propiedad intelectual y asignación de derecho de propiedad intelectual (ver 12.1.2), y protección de trabajos realizados en colaboración (ver también 6.1.3) ;
i) acuerdos de control de accesos que contemplen:
    1) los métodos de acceso permitidos, y el control y uso de identificadores únicos como IDs y contraseñas de usuarios;
    2) un proceso de autorización de acceso y privilegios de usuarios;
    3) un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso;
j) la definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;
k) el derecho a monitorear, y revocar (impedir), la actividad del usuario;
l) el derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías;
m) el establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia;
n) responsabilidades relativas a la instalación y el mantenimiento de hardware y software;
o) una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;
p) un proceso claro y detallado de administración de cambios;
q) los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;
r) los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;
s) los controles que garanticen la protección contra software malicioso (ver 8.3);
t) las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad;
u) la relación entre proveedores y subcontratistas.

4.3 Tercerización

Objetivo: Mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue delegada a otra organización.
Los acuerdos de tercerización deben contemplar los riesgos, los controles de seguridad y los procedimientos para sistemas de información, redes y/o ambientes de PC (desk top environments) en el contrato entre las partes.

4.3.1 Requerimientos de seguridad en contratos de tercerización

Los requerimientos de seguridad de una organización que terceriza la administración y el control de todos sus sistemas de información, redes y/o ambientes de PC, o de parte de los mismos, deben ser contemplados en un contrato celebrado entre las partes.

Entre otros ítems, el contrato debe contemplar:
a) cómo se cumplirán los requisitos legales, por ej., la legislación sobre protección de datos;
b) qué disposiciones se implementarán para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, estarán al corriente de sus responsabilidades en materia de seguridad;
c) cómo se mantendrá y comprobará la integridad y confidencialidad de los .activos de negocio de la organización ;

d) qué controles físicos y lógicos se utilizarán para restringir y delimitar el acceso de los usuarios autorizados a la información sensible de la organización;
e) cómo se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres;
f) qué niveles de seguridad física se asignarán al equipamiento tercerizado;
g) el derecho a la auditoría.

Asimismo, se deben tener en cuenta las cláusulas enumeradas en el punto 4.2.2 como parte de este contrato. El mismo debe permitir la ampliación de los requerimientos y procedimientos de seguridad en un plan de administración de la seguridad a ser acordado entre las partes.

Si bien los contratos de tercerización pueden plantear algunas cuestiones complejas en materia de seguridad, los controles incluidos en este código de práctica pueden servir como punto de partida para acordar la estructura y el contenido del plan de gestión de la seguridad.

5 CLASIFICACIÓN Y CONTROL DE ACTIVOS

5.1 Responsabilidad por rendición de cuentas de los activos

Objetivo: Mantener una adecuada protección de los activos de la organización.

Se debe rendir cuentas por todos los recursos de información importantes y se debe designar un propietario para cada uno de ellos.
La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. Se deben identificar a los propietarios para todos los activos importantes y se debe asignarse la responsabilidad por el mantenimiento de los controles apropiados. La responsabilidad por la implementación de los controles puede ser delegada. En último término, el propietario designado del activo debe rendir cuentas por el mismo.

5.1.1 Inventario de activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos de la empresa, como los relacionados con sanidad y seguridad, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un aspecto importante de la administración de riesgos. Una organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces,' asignar niveles de protección proporcionales al valor e importancia de los activos. , Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad (ver 5.2) deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño). Ejemplos de activos asociados a sistemas de información son los siguientes:

a) recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada;

b) recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
c) activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento ;
d) servicios: servicios informáticos y de comunicaciones, utilitarios generales, por ej., calefacción, iluminación, energía eléctrica, aire acondicionado.

5.2 Clasificación de la información

Objetivo: Garantizar que los recursos de información reciban un apropiado nivel de protección.
La información debe ser clasificada para señalar la necesidad, la prioridades y el grado de protección.
La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

5.2.1 Pautas de clasificación

Las clasificaciones y controles de protección asociados de la información, deben tomar cuenta de las necesidades de la empresa con respecto a la distribución (uso compartido) o restricción de la información, y de la incidencia de dichas necesidades en las actividades de la organización, por ej. acceso no autorizado o daño ala información. En general, la clasificación asignada a la información es una forma sencilla de señalar cómo ha de ser tratada y protegida. La información y las salidas de los sistemas que administran datos clasificados deben ser rotuladas según su valor y grado de sensibilidad para la organización. Asimismo, podría resultar conveniente rotular la información según su grado de criticidad, por ej. en términos de integridad y disponibilidad.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso ("over- classification") puede traducirse en gastos adicionales innecesarios para la organización. Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente, debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una política predeterminada (ver 9.1). Se debe considerar el número de categorías de clasificación y los beneficios que se obtendrán con su uso. Los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos. Deben interpretarse cuidadosamente los rótulos de clasificación de los documentos de otras organizaciones que podrían tener distintas definiciones para rótulos iguales o similares.

La responsabilidad por la definición de la clasificación de un ítem de información, por ej., un documento, registro de datos, archivo de datos o disquete, y por la revisión periódica de dicha clasificación, debe ser asignada al creador o propietario designado de la información.

5.2.2 Rotulado y manejo de la información

Es importante que se defina un conjunto de procedimientos adecuados para el rotulado y manejo de la información, según el esquema de clasificación adoptado por la organización. Estos procedimientos deben incluir los recursos de información en formatos físicos y electrónicos. Para cada

clasificación, se deben definir procedimientos de manejo que incluyan los siguientes tipos de actividades de procesamiento de la información:

a) copia;
b) almacenamiento;
c) transmisión por correo, fax y correo electrónico;
d) transmisión oral, incluyendo telefonía móvil, correo de voz, contestadores automáticos;

6 SEGURIDAD DEL PERSONAL

6.1 Seguridad en la definición de puestos de trabajo y la asignación de recursos

Objetivo : Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.
Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado.
Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados (ver 6.1.2), especialmente si se trata de tareas críticas. Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no revelación).

6.1.1 Inclusión de la seguridad en las responsabilidades de los puestos de trabajo

Las funciones y responsabilidades en materia de seguridad, según consta en la política de seguridad de la información de la organización (ver 3.1), deben ser documentadas según corresponda. Éstas deben incluir las responsabilidades generales por la implementación o el mantenimiento de la política de seguridad, así como las responsabilidades específicas por la protección de cada uno de los activos, o por la ejecución de procesos o actividades de seguridad específicos.

6.1.2 Selección y política de personal

Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto. Éstos deben incluir los siguientes:

a) disponibilidad de certificados de buena conducta satisfactorios, por ej. uno laboral y uno personal
b) una comprobación (de integridad y veracidad) del curriculum vitae del aspirante
c) constatación de las aptitudes académicas y profesionales alegadas
d) verificación de la identidad (pasaporte o documento similar).

Cuando un puesto, por asignación inicial o por promoción, involucra a una persona que tiene acceso a las instalaciones de procesamiento de información, y en particular si éstas manejan información sensible, por ej. información financiera o altamente confidencial, la organización también debe llevar a cabo una verificación de crédito. En el caso del personal con posiciones de jerarquía considerable, esta verificación debe repetirse periódicamente.

Un proceso de selección similar debe llevarse a cabo con contratistas y personal temporario. Cuando éste es provisto a través de una agencia, el contrato celebrado con la misma debe especificar claramente las responsabilidades de la agencia por la selección y los procedimientos de notificación que ésta debe seguir si la selección no ha sido efectuada o si los resultados originan dudas o inquietudes.

La gerencia debe evaluar la supervisión requerida para personal nuevo e inexperto con autorización para acceder a sistemas sensibles. El trabajo de todo el personal debe estar sujeto a revisión periódica y a procedimientos de aprobación por parte de un miembro del personal con mayor jerarquía.

Los gerentes deben estar al corriente de que las circunstancias personales de sus empleados pueden afectar su trabajo. Los problemas personales o financieros, los cambios en su conducta o estilo de vida, las ausencias recurrentes y la evidencia de stress o depresión pueden conducir a fraudes, robos, errores u otras implicaciones que afecten la seguridad. Esta información debe manejarse de acuerdo con la legislación pertinente que rija en la jurisdicción del caso.

6.1.3 Acuerdos de confidencialidad

Los acuerdos de confidencialidad o no divulgación se utilizan para reseñar que la información es confidencial o secreta. Los empleados deben firmar habitualmente un acuerdo de esta índole como parte de sus términos y condiciones iniciales de empleo.

El personal ocasional y los usuarios externos aún no contemplados en un contrato formalizado (que contenga el acuerdo de confidencialidad) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso a las instalaciones de procesamiento de información.

Los acuerdos de confidencialidad deben ser revisados cuando se producen cambios en los términos y condiciones de empleo o del contrato, en particular cuando el empleado está próximo a desvincularse de la organización o el plazo del contrato está por finalizar.

6.1.4 Términos y condiciones de empleo

Los términos y condiciones de empleo deben establecer la responsabilidad del empleado por la seguridad de la información. Cuando corresponda, estas responsabilidades deben continuar por un período definido una vez finalizada la relación laboral. Se deben especificar las acciones que se emprenderán si el empleado hace caso omiso de los requerimientos de seguridad.

Las responsabilidades y derechos legales del empleado, por ej. en relación con las leyes de derecho de propiedad intelectual o la legislación de protección de datos, deben ser clarificados e incluidos en los términos y condiciones de empleo.

También se debe incluir la responsabilidad por la clasificación y administración de los datos del empleador. Cuando corresponda, los términos y condiciones de empleo deben establecer que estas responsabilidades se extienden más allá de los límites de la sede de la organización y del horario normal de trabajo, por ej. cuando el empleado desempeña tareas en su domicilio (ver también 7.2.5 y 9.8.1).

6.2 Capacitación del usuario

Objetivo : Garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus tareas normales.
Los usuarios deben ser capacitados en relación con los procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad.

6.2.1 Formación y capacitación en materia de seguridad de la información

Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles del negocio, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, por ej. el procedimiento de entrada al sistema ("log-on") y el uso de paquetes de software, antes de que se les otorgue acceso a la información o a los servicios.

6.3 Respuesta a incidentes y anomalías en materia de seguridad

Objetivo : Minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos.
Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible.
Se debe concientizar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la organización. Se debe requerir que los mismos comuniquen cualquier incidente advertido o supuesto al punto de contacto designado tan pronto como sea posible. La organización debe establecer un proceso disciplinario formal para ocuparse de los empleados que perpetren violaciones de la seguridad. Para lograr abordar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto como sea posible una vez ocurrido el hecho (ver 12.1.7).

6.3.1 Comunicación de incidentes relativos a la seguridad

Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible.

Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca la acción que ha de emprenderse al recibir un informe sobre incidentes. Todos los empleados y contratistas deben estar al corriente del procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto como sea posible.

Deberán implementarse adecuados procesos de "feedback" para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos los mismos.

Estos incidentes pueden ser utilizados durante la capacitación a fin de crear conciencia de seguridad en el usuario (ver 6.2) como ejemplos de lo que puede ocurrir, de cómo responder a dichos incidentes y de cómo evitarlos en el futuro (ver también 12.1.7).

6.3.2 Comunicación de debilidades en materia de seguridad

Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.

Deberán comunicar estos asuntos a su gerencia, o directamente a su proveedor de servicios, tan pronto como sea posible. Se debe informar a los usuarios que ellos no deben, bajo ninguna circunstancia, intentar probar una supuesta debilidad. Esto se lleva a cabo para su propia protección, debido a que el intentar probar debilidades puede ser interpretado como un potencial mal manejo del sistema.

6.3.3 Comunicación de anomalías del software

Se deben establecer procedimientos para la comunicación de anomalías del software. Se deben considerar las siguientes acciones:

a) Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en pantalla.
b) La computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato a la persona pertinente (contacto). Si se ha de examinar el equipo, éste debe ser desconectado de las redes de la organización antes de ser activado nuevamente. Los disquetes no deben transferirse a otras computadoras.
c) El asunto debe ser comunicado inmediatamente al gerente de seguridad de la información.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados a hacerlo. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

6.3.4 Aprendiendo de los incidentes

Debe haberse implementado mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información debe utilizarse para identificar incidentes o anomalías recurrentes o de alto impacto. Esto puede señalar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros, o de tomarlos en cuenta en el proceso de revisión de la política de seguridad (ver 3.1.2).

6.3.5 Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización (ver 6.1.4 y para el tópico retención de evidencia, ver 12.1.7). Dicho proceso puede servir de factor disuasivo de los empleados que, de no mediar el mismo, podrían ser proclives a pasar por alto los procedimientos de seguridad.

Asimismo, este proceso debe garantizar un trato imparcial y correcto hacia los empleados sospechosos de haber cometido violaciones graves o persistentes a la seguridad.

7 SEGURIDAD FÍSICA Y AMBIENTAL

7.1 Áreas seguras

Objetivo: Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.
Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.
La protección provista debe ser proporcional a los riesgos identificados. Se recomienda la implementación políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información.

7.1.1 Perímetro de seguridad física

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.

Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información (ver 7.1.3). Un perímetro de seguridad es algo delimitado por una barrera, por ej. una pared, una puerta de acceso controlado por tarjeta o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos.
Se deben considerar e implementar los siguientes lineamientos y controles, según corresponda.

a) El perímetro de seguridad debe estar claramente definido.
b) El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente sólido (por ej. no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
c) Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.
d) Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.
e) Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

7.1.2 Controles de acceso físico

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.
c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.
d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

7.1.3 Protección de oficinas, recintos e instalaciones

Un área protegida puede ser una oficina cerrada con llave, o diversos recintos dentro de un perímetro de seguridad física, el cual puede estar bloqueado y contener cajas fuertes o gabinetes con cerraduras. Para la selección y el diseño de un área protegida debe tenerse en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También deben tomarse en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se deberán considerar las amenazas a la seguridad que representan los edificios y zonas aledañas, por ej. filtración de agua desde otras áreas.

Se deben considerar los siguientes controles

a) Las instalaciones clave deben ubicarse en lugares a los cuales no pueda acceder el público.
b) Los edificios deben ser discretos y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores, que identifiquen la presencia de actividades de procesamiento de información.
c) Las funciones y el equipamiento de soporte, por ej. fotocopiadoras, máquinas de fax, deben estar ubicados adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
d) Las puertas y ventanas deben estar bloqueadas cuando no hay vigilancia **y** debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular las que se encuentran al nivel del suelo.
e) Se deben implementar adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles. Las áreas vacías deben tener alarmas activadas en todo momento. También deben protegerse otras áreas, como la sala de cómputos o las salas de comunicaciones.
f) Las instalaciones de procesamiento de información administradas por la organización deben estar físicamente separadas de aquellas administradas por terceros.
g) Los guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible no deben ser fácilmente accesibles al público.
h) Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área protegida. Los suministros a granel, como los útiles de escritorio, no deben ser almacenados en el área protegida hasta que sean requeridos.
i) El equipamiento de sistemas de soporte UPC (Usage Parameter Control) de reposición de información perdida ("fallback") y los medios informáticos de resguardo deben estar situados a una distancia prudencial para evitar daños ocasionados por eventuales desastres en el sitio principal.

7.1.4 Desarrollo de tareas en áreas protegidas

Para incrementar la seguridad de un área protegida pueden requerirse controles y lineamientos adicionales. Esto incluye controles para el personal o terceras partes que trabajan en el área protegida, así como para las actividades de terceros que tengan lugar allí. Se deberán tener en cuenta los siguientes puntos:

a) El personal sólo debe tener conocimiento de la existencia de un área protegida, o de las actividades que se llevan a cabo dentro de la misma, según el criterio de necesidad de conocer.
b) Se debe evitar el trabajo no controlado en las áreas protegidas tanto por razones de seguridad como para evitar la posibilidad de que se lleven a cabo actividades maliciosas.

c) Las áreas protegidas desocupadas deben ser físicamente bloqueadas y periódicamente inspeccionadas.
d) El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
e) A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de vídeo, audio u otro tipo de equipamiento que registre información.

7.1.5 Aislamiento de las áreas de entrega y carga

Las áreas de entrega y carga deben ser controladas y, si es posible, estar aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos. Se deben tener en cuenta los siguientes lineamientos:

a) El acceso a las áreas de depósito, desde el exterior de la sede de la organización, debe estar limitado a personal que sea previamente identificado y autorizado.
b) El área de depósito debe ser diseñada de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Todas las puertas exteriores de un área de depósito deben ser aseguradas cuando se abre la puerta interna.
d) El material entrante debe ser inspeccionado para descartar peligros potenciales (ver 7.2.l d) antes de ser trasladado desde el área de depósito hasta el lugar de uso.
e) El material entrante debe ser registrado, si corresponde (ver 5.1), al ingresar al sitio pertinente.

7.2 Seguridad del equipamiento

Objetivo: Impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa.
El equipamiento debe estar físicamente protegido de las amenazas a la seguridad y los peligros del entorno
Es necesaria la protección del equipamiento (incluyendo el que se utiliza en forma externa) para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Esto también debe tener en cuenta la ubicación y disposición equipamiento. Pueden requerirse controles especiales para prevenir peligros o accesos no autorizados, y para proteger instalaciones de soporte, como la infraestructura de cableado y suministro de energía eléctrica.

7.2.1 Ubicación y protección del equipamiento

El equipamiento debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. Se deben tener en cuenta los siguientes puntos:

a) El equipamiento debe ser ubicado en un sitio que permita minimizar el acceso innecesario a las áreas de trabajo.
b) Las instalaciones de procesamiento y almacenamiento de información, que manejan datos sensibles, deben ubicarse en un sitio que permita reducir el riesgo de falta de supervisión de las mismas durante su uso.

c) Los ítems que requieren protección especial deben ser aislados para reducir el nivel general de protección requerida.
d) Se deben adoptar controles para minimizar el riesgo de amenazas potenciales, por ej.
    1) robo
    2) incendio
    3) explosivos
    4) humo;
    5) agua (o falta de suministro)
    6) polvo
    7) vibraciones
    8) efectos químicos
    9) interferencia en el suministro de energía eléctrica.
    10) radiación electromagnética.

e) La organización debe analizar su política respecto de comer, beber y fumar cerca de las instalaciones de procesamiento de información.
f) Se deben monitorear las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.
g) Se debe tener en cuenta el uso de métodos de protección especial, como las membranas de teclado, para los equipos ubicados en ambientes industriales.
h) Se debe considerar el impacto de un eventual desastre que tenga lugar en zonas próximas a la sede de la organización, por ej. un incendio en un edificio cercano, la filtración de agua desde el cielo raso o en pisos por debajo del nivel del suelo o una explosión en la calle.

7.2.2 Suministros de energía

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. Se debe contar con un adecuado suministro de energía que esté de acuerdo con las especificaciones del fabricante o proveedor de los equipos. Entre las alternativas para asegurar la continuidad del suministro de energía podemos enumerar las siguientes:

a) múltiples bocas de suministro para evitar un único punto de falla en el suministro de energía
b) suministro de energía ininterrumpible (UPS)
c) generador de respaldo.

Se recomienda una UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la organización. Los planes de contingencia deben contemplar las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.

Se debe tener en cuenta el empleo de un generador de respaldo si el procesamiento ha de continuar en caso de una falla prolongada en el suministro de energía. De instalarse, los generadores deben ser probados periódicamente de acuerdo con las instrucciones del fabricante o proveedor. Se debe disponer de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.

Asimismo, los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se debe implementar protección contra rayos en todos los edificios y se deben adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.

7.2.3 Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño. Se deben tener en cuenta los siguientes controles:

a) Las líneas de energía eléctrica y telecomunicaciones que se conectan con las instalaciones de procesamiento de información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa.
b) El cableado de red debe estar protegido contra interceptación no autorizada o daño, por ejemplo mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas.
c) Los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias.
d) Entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes
    1) instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
    2) uso de rutas o medios de transmisión alternativos
    3) uso de cableado de fibra óptica
    4) iniciar barridos para eliminar dispositivos no autorizados conectados a los cables.

7.2.4 Mantenimiento de equipos

El equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes. Se deben considerar los siguientes lineamientos:

a) El equipamiento debe mantenerse de acuerdo con los intervalos servicio y especificaciones recomendados por el proveedor.
b) Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.
e) Deben implementarse controles cuando se retiran equipos de la sede de la organización para su mantenimiento (ver también 7.2.6 con respecto a borrado, borrado permanente y sobre escritura de datos). Se debe cumplir con todos los requisitos impuestos por las pólizas de seguro.

7.2.5 Seguridad del equipamiento fuera del ámbito de la organización

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la organización, debe ser autorizado por el nivel gerencial, sin importar quien es el propietario del mismo. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la organización, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento de procesamiento de la información incluye todo tipo de computadoras personales, organizadores, teléfonos móviles, papel u otros formularios, necesarios para el trabajo en el domiciliario o que es transportado fuera del lugar habitual de trabajo.

Se deben considerar los siguientes lineamientos:

a) El equipamiento y dispositivos retirados del ámbito de la organización no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano y de ser posible enmascaradas, durante el viaje.

b) Se deben respetar permanentemente las instrucciones del fabricante, por ej. protección por exposición a campos electromagnéticos fuertes.
c) Los controles de trabajo en domicilio deben ser determinados a partir de un análisis de riesgo y se aplicarán controles adecuados según corresponda, por ej. gabinetes de archivo con cerradura, política de escritorios limpios y control de acceso a computadoras.
d) Una adecuada cobertura de seguro debe estar en orden para proteger el equipamiento fuera del ámbito de la organización.

Los riesgos de seguridad, por ej. el daño, robo o escucha subrepticia, pueden variar considerablemente según las ubicaciones y deben ser tenidas en cuenta al determinar los controles más apropiados. Se puede encontrar más información sobre otros aspectos de protección del equipamiento móvil, en 9.8.1

7.2.6 Baja segura o reutilización de equipamiento.

La información puede verse comprometida por una desafectación descuidada o una reutilización del equipamiento (véase también 8.6.4). Los medios de almacenamiento conteniendo material sensitivo, deben ser físicamente destruidos o sobrescritos en forma segura en vez de utilizar las funciones de borrado estándar.

Todos los elementos del equipamiento que contengan dispositivos de almacenamiento, por ej. discos rígidos no removibles, deben ser controlados para asegurar que todos los datos sensitivos y el software bajo licencia, han sido eliminados o sobrescritos antes de su baja. Puede ser necesario realizar un análisis de riesgo a fin de determinar si medios de almacenamiento dañados, conteniendo datos sensitivos, deben ser destruidos, reparados o desechados.

7.3 Controles generales

Objetivo : Impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma.
Las instalaciones de procesamiento de la información y la información deben ser protegidas contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños. Los procedimientos de administración y almacenamiento son considerados en el punto 8.6.3.

7.3.1 Políticas de escritorios y pantallas limpias.

Las organizaciones deben considerar la adopción de una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

La política debe contemplar las clasificaciones de seguridad de la información (ver 5.2), los riesgos correspondientes y los aspectos culturales de la organización.

La información que se deja sobre los escritorios también está expuesta a sufrir daños o destrozos en caso de producirse un desastre como incendio, inundación o explosión.

Se deben aplicar los siguientes lineamientos.

a) Cuando corresponda, los documentos en papel y los medios informáticos deben ser almacenados bajo llave en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
b) La información sensible o crítica de la empresa debe guardarse bajo llave (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina
c) Las computadoras personales, terminales e impresoras no deben dejarse conectadas cuando están desatendidas y las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso.
d) Se deben proteger los puntos de recepción y envío de correo y las máquinas de fax y telex no atendidas
e) Las fotocopiadoras deben estar bloqueadas (o protegidas de alguna manera, del uso no autorizado) fuera del horario normal de trabajo,
f) La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

7.3.2 Retiro de bienes

El equipamiento, la información o el software no deben ser retirados de la sede de la organización sin autorización. Cuando sea necesario y procedente, los equipos deberán ser desconectados ("logged out") y nuevamente conectados ("logged in") cuando se reingresen. Se deben llevar a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la organización. El personal debe conocer la posibilidad de realización de dichas comprobaciones.

8 GESTIÓN DE COMUNICACIONES Y OPERACIONES

8.1 Procedimientos y responsabilidades operativas

Objetivo: Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidentes.
Se debe implementar la separación de funciones (ver 8.1.4), cuando corresponda, a fin de reducir el riesgo del uso negligente o mal uso deliberado del sistema.

8.1.1 Documentación de los procedimientos operativos

Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.

Los procedimientos deben especificar las instrucciones para la ejecución detallada de cada tarea, con inclusión de:

a) procesamiento y manejo de la información
b) requerimientos de programación ("schedulling"), incluyendo interdependencias con otros sistemas, tiempos de inicio de primeras tareas y tiempos de terminación de últimas tareas;

c) instrucciones para el manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución de tareas, incluyendo restricciones en el uso de utilitarios del sistema (ver 9.5.5)
d) personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas
e) instrucciones especiales para el manejo de salidas ("outputs"), como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas de tareas fallidas
f) reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

También debe prepararse documentación sobre procedimientos referidos a actividades de mantenimiento del sistema, relacionadas con las instalaciones de procesamiento de información y comunicaciones, tales como los procedimientos de inicio y cierre, resguardo, mantenimiento de equipos, salas de cómputos y administración y seguridad del manejo de correo.

8.1.2 Control de cambios en las operaciones

Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información. El control inadecuado de estos cambios es una causa común de las fallas de seguridad y de sistemas.

Se deben implementar responsabilidades y procedimientos gerenciales formales para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software o los procedimientos. Los programas operativos deben estar sujetos a un control estricto de los cambios. Cuando se cambian los programas, se debe retener un registro de auditoría que contenga toda la información relevante.

Los cambios en el ambiente operativo pueden tener impacto en las aplicaciones. Siempre que sea factible, los procedimientos de control de cambios en las operaciones y aplicaciones deben estar integrados (ver también 10.5.1). En particular, se deben considerar los siguientes ítems:

a) identificación y registro de cambios significativos
b) evaluación del posible impacto de dichos cambios
c) procedimiento de aprobación formal de los cambios propuestos
d) comunicación de detalles de cambios a todas las personas pertinentes
e) procedimientos que identifican las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

8.1.3 Procedimientos de manejo de incidentes

Se deben establecer responsabilidades y procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad (ver también 6.3. l).

Se deben considerar los siguientes controles.

a) Se deben establecer procedimientos que contemplen todos los tipos probables de incidentes relativos a seguridad, incluyendo
    1) fallas en los sistemas de información y pérdida del servicio;
    2) negación del servicio;
    3) errores ocasionados por datos comerciales incompletos o inexactos;
    4) violaciones de la confidencialidad;
b) Además de los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible), los procedimientos también deben contemplar (ver también 6.3.4):
    1) análisis e identificación de la causa del incidente;

2) planificación e implementación de soluciones para evitar la repetición del mismo, si resulta necesario;
3) recolección de pistas de auditoría y evidencia similar;
4) comunicación con las personas afectadas o involucradas con la recuperación, del incidente;
5) notificación de la acción a la autoridad pertinente;

c) Se deben recolectar (ver 12.1.7) y proteger pistas de auditoría y evidencia similar, según corresponda, para:
1) análisis de problemas internos:
2) uso como evidencia en relación con una probable violación de contrato, de requisito normativo, o en el caso de un proceso judicial civil o criminal, por ej. por aplicación de legislación sobre protección de datos o fraude informático;
3) negociación de compensaciones por parte de los proveedores de software y de servicios;

d) Se deben implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema. Los procedimientos deben garantizar que :
1) sólo se otorga acceso a los sistemas y datos existentes al personal claramente identificado y autorizado (ver también 4.2.2 en relación con el acceso de terceros);
2) todas las acciones de emergencia emprendidas son documentadas en forma detallada
3) la acciones de emergencia se comunican a la gerencia y se revisan sistemáticamente;
4) la integridad de los controles y sistemas de la empresa se constata en un plazo mínimo.

8.1.4 Separación de funciones

La separación de funciones es un método para reducir el riesgo de mal uso, accidental o deliberado del sistema. Se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios.

Las pequeñas organizaciones pueden encontrar este método de control difícil de cumplir, pero el principio debe aplicarse en la medida de lo posible. Siempre que sea difícil llevar a cabo la separación, se deben tener en cuenta otros controles como el monitoreo de las actividades, las pistas de auditoría y la supervisión gerencial. Es importante que la auditoría de seguridad permanezca independiente. Se deben tomar recaudos para que ninguna persona pueda perpetrar un fraude en áreas de responsabilidad única sin ser detectada. El inicio de un evento debe estar separado de su autorización. Se deben considerar los siguientes puntos.

a) Es importante separar actividades que requieren connivencia para defraudar, por ej. efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Si existe peligro de connivencia, los controles deben ser diseñados de manera tal que dos o más personas deban estar involucradas, reduciendo de ese modo la posibilidad de conspiración.

8.1.5 Separación entre instalaciones de desarrollo e instalaciones operativas

La separación entre las instalaciones de desarrollo, prueba y operaciones es importante para lograr la separación de los roles involucradas. Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Las actividades de desarrollo y prueba pueden ocasionar problemas graves, como la modificación no deseada de archivos o sistemas, o la rectificación no deseada de fallas de sistemas. Se debe consi-

derar el nivel de separación que resulta necesario entre los ambientes operativos, de prueba y de desarrollo, a fin de prevenir problemas operativos. También se debe implementar una separación similar entre las funciones de desarrollo y prueba. En este caso, existe la necesidad de mantener un ambiente conocido y estable en el cual puedan llevarse a cabo pruebas significativas e impedirse accesos inadecuados por parte del personal de desarrollo.

Si el personal de desarrollo y prueba tiene acceso al sistema que esta operativo y a su información, éste puede ser capaz de introducir líneas de códigos no autorizados o no probados, o alterar los datos de las operaciones. En algunos sistemas esta capacidad puede ser utilizada inadecuadamente para perpetrar fraude, o para introducir programas no probados o maliciosos. Estos programas pueden ocasionar graves problemas operativos. El personal de desarrollo y pruebas también plantea una amenaza a la confidencialidad de la información operativo.

Las actividades de desarrollo y pruebas pueden producir cambios no planificados en el software y la información si los sistemas comparten el mismo ambiente informático. La separación entre las instalaciones de desarrollo, pruebas y operaciones es por tanto deseable, a fin de reducir el riesgo de cambios accidentales o accesos no autorizados al software operativo y a los datos del negocio. Se deben tener en cuenta los siguientes controles.

a) El software en desarrollo y en operaciones debe, en la medida de lo posible, ejecutarse en diferentes procesadores o en diferentes dominios o directorios.
b) En la medida de lo posible, las actividades de desarrollo y prueba deben estar separadas.
c) Cuando no es requerido, los compiladores, editores y otros utilitarios del sistema no deben ser accesibles desde los sistemas que están operativos.
d) Se deben utilizar diferentes procedimientos de conexión ("log-on") para sistemas en operaciones y de prueba, a fin de reducir el riesgo de error. Se debe alentar a los usuarios a utilizar diferentes contraseñas para estos sistemas, y los menús deben desplegar adecuados mensajes de identificación.
e) El personal de desarrollo sólo debe tener acceso a las contraseñas operativas, porque allí están adecuadamente ubicados los controles de emisión de contraseñas para el apoyo de los sistemas que se encuentran operativos. Estos controles deben garantizar que dichas contraseñas se modifiquen una vez utilizadas.

8.1.6 Administración de instalaciones externas

El empleo de un contratista externo para la administración de las instalaciones de procesamiento de información puede introducir potenciales exposiciones al riesgo en materia de seguridad, como la posibilidad de compromiso, daño o pérdida de datos en la sede del contratista. Estos riesgos deben ser identificados con anticipación, y deben acordarse controles adecuados con el contratista e incluirse en el contrato (ver también 4.2.2 y 4.3 para orientación con respecto a contratos con terceros que contemplan el acceso a instalaciones de la organización y contratos de tercerización)

Se deben abordar, entre otras, las siguientes cuestiones específicas:

a) identificar las aplicaciones sensibles o críticas que convienen retener en la organización;
b) obtener la aprobación de los propietarios de aplicaciones comerciales;
c) implicancias para la continuidad de los planes comerciales;
d) estándares de seguridad a especificar, y el proceso de medición del cumplimiento;
e) asignación de responsabilidades específicas y procedimientos para monitorear con eficacia todas las actividades de seguridad pertinentes
f) responsabilidades y procedimientos de comunicación y manejo de incidentes relativos a la seguridad (ver 8.1.3).

8.2 Planificación y aprobación de sistemas

Objetivo : Minimizar el riesgo de fallas en los sistemas.
Se requiere una planificación y preparación anticipada para garantizar la disponibilidad de capacidad y recursos adecuados.
Deben realizarse proyecciones para futuros requerimientos de capacidad, a fin de reducir el riesgo de sobrecarga del sistema. Se deben establecer, documentar y probar los requerimientos operativos de nuevos sistemas antes de su aprobación y uso.

8.2.1 Planificación de la capacidad

Se deben monitorear las demandas de capacidad y realizar proyecciones de los futuros requerimientos de capacidad, a fin de garantizar la disponibilidad del poder de procesamiento y almacenamiento adecuados. Estas proyecciones deben tomar en cuenta los nuevos requerimientos de negocios y sistemas y las tendencias actuales y proyectadas en el procesamiento de la información de la organización.

Las computadoras "mainframe" requieren especial atención, debido al mayor costo y plazo de espera para la obtención de nueva capacidad. Los administradores de servicios mainframe deben monitorear la utilización de los recursos clave del sistema, incluyendo procesadores, almacenamiento principal, almacenamiento de archivos, impresoras y otros medios de salida ("output"), y sistemas de comunicaciones. Éstos deben identificar las tendencias de uso, particularmente en relación con las aplicaciones comerciales o las herramientas de sistemas de información de gestión.

Los gerentes deben utilizar esta información para identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad del sistema o a los servicios del usuario, y planificar una adecuada acción correctiva..

8.2.2 Aprobación del sistema

Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones ("upgrades") y nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación. Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados. Se deben considerar los siguientes puntos:

a) desempeño y requerimientos de capacidad de las computadoras;
b) recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
c) preparación y prueba de procedimientos operativos de rutina según estándares definidos
d) conjunto acordado de controles de seguridad implementados
e) procedimientos manuales eficaces;
f) disposiciones relativas a la continuidad de los negocios, según lo requerido en el punto 11.1
g) evidencia que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como durante los últimos días del mes
h) evidencia de que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad global de la organización
i) entrenamiento en la operación o uso de nuevos sistemas.

Para los principales nuevos desarrollos, las funciones y usuarios de operaciones deben ser consultados en todas las etapas del proceso de desarrollo para garantizar la eficiencia operativa del diseño propuesto del sistema. Deben llevarse a cabo pruebas apropiadas para constatar el cumplimiento cabal de todos los criterios de aprobación.

8.3 Protección contra software malicioso

Objetivo : Proteger la integridad del software y la información.
Es necesario tomar precauciones para prevenir y detectar la introducción de software malicioso.
El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso como, por ej., virus informáticos, "worms" de red, "troyanos" (ver también 10.5.4) y bombas lógicas. Se debe concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso, y los administradores deben, cuando corresponda, introducir controles especiales para detectar o prevenir la introducción de los mismos. En particular, es esencial que se tomen precauciones para detectar y prevenir virus informáticos en computadoras personales.

8.3.1 Controles contra software malicioso

Se deben implementar controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de usuarios. La protección contra software malicioso debe basarse en la concientización en materia de seguridad y en controles adecuados de acceso al sistema y administración de cambios.

Se deben tener en cuenta los siguientes controles:

a) una política formal que requiera el uso de software con licencia y prohíba el uso de software no autorizado (ver 12.1.2.2);
b) una política formal con el fin de proteger contra los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando qué medidas de protección deberían tomarse (ver también 10.5, especialmente 10.5.4 y 1 0.5.5);
c) instalación y actualización periódica de software de detección y reparación anti-virus, para examinar computadoras y medios informáticos, ya sea como medida precautoria o rutinaria,
d) realización de revisiones periódicas del contenido de software y datos de los sistemas que sustentan procesos críticos de al empresa. La presencia de archivos no aprobados o modificaciones no autorizadas debe ser investigada formalmente;
e) verificación de la presencia de virus en archivos de medios electrónicos de origen incierto o no autorizado, o en archivos recibidos a través de redes no confiables, antes de su uso;
f) verificación de la presencia de software malicioso en archivos adjuntos a mensajes de correo electrónico y archivos descargados por Internet ("downloads") antes de su uso. Esta verificación puede llevarse a cabo en diferentes lugares, por ej. en servidores de correo electrónico, computadoras de escritorio o al ingresar en la red de la organización;
g) procedimientos y responsabilidades gerenciales para administrar la protección contra virus en los sistemas, el entrenamiento con respecto a su uso, la comunicación y la recuperación frente a ataques (ver 6.3 y 8.1.3)
h) adecuados planes de continuidad de los negocios para la recuperación respecto de ataques de virus, incluyendo todos los datos necesarios, el resguardo del software y las disposiciones para la recuperación (ver el punto 11)
i) procedimientos para verificar toda la información relativa a software malicioso, y garantizar que los boletines de alerta sean exactos e informativos. Los gerentes deben garantizar que se utilizan fuentes calificadas, por ej. publicaciones acreditadas, sitios de Internet o proveedores de software anti-virus confiables, para diferenciar entre virus falaces y reales. Se debe concientizar al personal acerca del problema de los virus falsos (hoax) y de qué hacer al recibirlos.

Estos controles son especialmente importantes para servidores de archivos de red que brindan soporte a un gran número de estaciones de trabajo.

8.4 Mantenimiento

Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento y comunicación de información.
Se deben establecer procedimientos de rutina para llevar a cabo la estrategia de resguardo acordada (ver 11.1) realizando copias de resguardo de los datos y ensayando su restablecimiento oportuno, registrando eventos y fallas y, cuando corresponda, monitoreando el entorno del equipamiento.

8.4.1 Resguardo de la información

Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la empresa. Se debe contar con adecuadas instalaciones de resguardo para garantizar que toda la información y el software esencial de la empresa puede recuperarse una vez ocurrido un desastre o falla de los dispositivos. Las disposiciones para el resguardo de cada uno de los sistemas deben ser probadas periódicamente para garantizar que cumplen con los requerimientos de los planes de continuidad de los negocios (ver punto 11). Se deben tener en cuenta los siguientes controles.

a) Se debe almacenar en una ubicación remota un nivel mínimo de información de resguardo, junto con registros exactos y completos de las copias de resguardo y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres generaciones o ciclos de información de resguardo para aplicaciones importantes de la empresa.
b) Se debe asignar a la información de resguardo un nivel adecuado de protección física y ambiental (ver punto 7) consecuente con los estándares aplicados en el sitio principal. Los controles aplicados a los dispositivos en el sitio principal deben extenderse para cubrir el sitio de resguardo.
c) Los medios de resguardo deben probarse periódicamente, cuando sea factible, a fin de garantizar la confiabilidad de los mismos con relación a su eventual uso en casos de emergencia.
d) Los procedimientos de restauración deben verificarse y probarse periódicamente para garantizar su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Se debe determinar el período de guarda de la información esencial para la empresa, y también los requerimientos de copias de archivos que han de guardarse en forma permanente (ver 12.1.3).

8.4.2 Registro de actividades del personal operativo

El personal operativo debe mantener un registro de sus actividades. Los registros deben incluir, según corresponda:

a) tiempos de inicio y cierre del sistema
b) errores del sistema y medidas correctivas tomadas
c) confirmación del manejo correcto de archivos de datos y salidas
d) el nombre de la persona que lleva a cabo la actualización del registro

Los registros de actividades del personal operativo deben estar sujetos a verificaciones periódicas e independientes con relación a los procedimientos operativos.

8.4.3 Registro de fallas

Se deben comunicar las fallas y tomar medidas correctivas. Se debe registrar las fallas comunicadas por los usuarios, con respecto a problemas con el procesamiento de la información o los sistemas de

comunicaciones. Deben existir reglas claras para el manejo de las fallas comunicadas, con inclusión de:

a) revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente
b) revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron debidamente autorizadas.

8.5 Administración de la red

Objetivo: Garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo. Es de suma importancia la administración de seguridad de las redes que pueden atravesar el perímetro de la organización.
También pueden requerirse controles adicionales para los datos sensibles que circulen por redes públicas.

8.5.1 Controles de redes

Se requiere un conjunto de controles para lograr y mantener la seguridad de las redes informáticas. Los administradores de redes deben implementar controles para garantizar la seguridad de los datos en la misma, y la protección de los servicios conectados contra el acceso no autorizado, En particular, se deben considerar los siguientes ítems.

a) Cuando corresponda, la responsabilidad operativa de las redes debe estar separada de las de operaciones del computador (ver 8.1.4).
b) Se deben establecer los procedimientos y responsabilidades para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias
c) Si resulta necesario, deben establecerse controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados (ver 9.4 y 10.3). También pueden requerirse controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
d) Las actividades gerenciales deben estar estrechamente coordinadas tanto para optimizar el servicio a la actividad de la empresa cuanto para garantizar que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

8.6 Administración y seguridad de los medios de almacenamiento

Objetivo : Impedir el daño a los activos y las interrupciones en las actividades de la empresa.
Los medios de almacenamiento deben ser controlados y protegidos físicamente. Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, casetes), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado.

8.6.1 Administración de medios informáticos removibles

Deben existir procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. Se deben considerar los siguientes lineamientos:

a) si ya no son requeridos, deben borrarse los contenidos previos de cualquier medio reutilizable que ha de ser retirado de la organización.

b) Se debe requerir autorización para retirar cualquier medio de la organización y se debe realizar un registro de todos los retiros a fin de mantener una pista de auditoría (ver 8.7.2).
c) Todos los medios deben almacenarse en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Todos los procedimientos y niveles de autorización deben ser claramente documentados.

8.6.2 Eliminación de medios informáticos

Cuando ya no son requeridos, los medios informáticos deben eliminarse de manera segura. Si los mismos no se eliminan cuidadosamente, la información sensible puede filtrarse a personas ajenas a la organización. Se deben establecer procedimientos formales para la eliminación segura de los medios informáticos, a fin de minimizar este riesgo. Deben considerarse los siguientes controles.

a) Los medios que contienen información sensible deben ser almacenados y eliminados de manera segura, por ej. incinerándolos o haciéndolos trizas, o eliminando los datos y utilizando los medios en otra aplicación dentro de la organización.
b) El siguiente listado identifica ítems que podrían requerir una eliminación segura:
    1) documentos en papel,
    2) voces u otras grabaciones;
    3) papel carbónico;
    4) informes de salida,
    5) cintas de impresora de un solo uso;
    6) cintas magnéticas;
    7) discos o casetes removibles;
    8) medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor);
    9) listados de programas;
    10) datos de prueba;
    11) documentación del sistema,
c) Puede resultar más fácil disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.
d) Muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipos y medios. Se debe seleccionar cuidadosamente a un contratista apto con adecuados controles y experiencia.
e) Cuando sea posible, se debe registrar la eliminación de los ítems sensibles, a fin de mantener una pista de auditoría.

Al acumular medios para su eliminación, se debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

8.6.3 Procedimientos de manejo de la información

Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada. Los procedimientos de manejo de información deben elaborarse según la clasificación de la misma (ver 5.2) en documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem sensible, por ej. facturas y cheques en blanco. Se deben tener en cuenta los siguientes controles (ver también 5.2 y 8.7.2):

a) manejo y rotulado de todos los medios (ver también 8.7.2 a);

b) restricción de acceso para identificar al personal no autorizado;
c) mantenimiento de un registro formal de los receptores autorizados de datos;
d) garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se aplica la validación de salidas;
e) protección de datos en espera ("spooled data") en un nivel consecuente con el grado de sensibilidad de los mismos
f) almacenamiento de medios en un ambiente que concuerda con las especificaciones de los fabricantes o proveedores
g) mantener la distribución de datos en un nivel mínimo
h) marcación clara de todas las copias de datos a fin de ser advertidas por el receptor autorizado
i) revisión de listados de distribución y listados de receptores autorizados a intervalos regulares.

8.6.4 Seguridad de la documentación del sistema

La documentación del sistema puede contener cierta cantidad de información sensible, por ej. descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización (ver también 9.1). Se deben considerar los siguientes controles para proteger la documentación del sistema de accesos no autorizados.

a) La documentación del sistema debe ser almacenada en forma segura;
b) El listado de acceso a la documentación del sistema debe restringirse al mínimo y debe ser autorizado por el propietario de la aplicación;
c) La documentación del sistema almacenada en una red pública, o suministrada a través de una red pública, debe ser protegida de manera adecuada;

8.7 Intercambios de información y software

Objetivo: Impedir la pérdida, modificación o uso inadecuado de la información que intercambian las organizaciones.
Los intercambios de información y software entre organizaciones deben ser controlados, y deben ser consecuentes con la legislación aplicable (ver punto 12). Los intercambios deben llevarse a cabo de conformidad con los acuerdos existentes. Se deben establecer procedimientos y estándares para proteger la información y los medios en tránsito. Se deben considerar las implicancias comerciales y de seguridad relacionadas con el intercambio electrónico de datos, el comercio electrónico y el correo electrónico, además de los requerimientos de controles.

8.7.1 Acuerdos de intercambio de información y software

Se deben establecer acuerdos, algunos de los cuales pueden ser formales, incluyendo los acuerdos de custodia de software cuando corresponda, para el intercambio de información y software (tanto electrónico como manual) entre organizaciones. Las especificaciones de seguridad de los acuerdos de esta índole deben reflejar el grado de sensibilidad de la información de negocio involucrada. Los acuerdos sobre requisitos de seguridad deben tener en cuenta

a) responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones ;
b) procedimientos de notificación de emisor, transmisión, envío y recepción;
c) estándares técnicos mínimos para armado de paquetes y transmisión;
d) estándares de identificación de mensajeros (“courier”);
e) responsabilidades y obligaciones en caso de pérdida de datos
f) uso de un sistema convenido para el rotulado de información crítica o sensible, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida;

g) información sobre la propiedad de la información y el software, y responsabilidades por la protección de los datos, el cumplimiento del "derecho de propiedad intelectual" del software y consideraciones similares (ver 12.1.2 y 12.1.4) ;
1

h) estándares técnicos para la grabación y lectura de la información y software ;
i) controles especiales que pueden requerirse para proteger ítems sensibles, como las claves criptográficas (ver 10.3.5).

8.7.2 Seguridad de los medios en tránsito

La información puede ser vulnerable a accesos no autorizados, mal uso o alteración durante el transporte físico, por ejemplo cuando se envían medios a través de servicios postales o de mensajería.

Los siguientes controles deben ser aplicados para salvaguardar los medios informáticos que se transportan entre distintos puntos.

a) Se deben utilizar medios de transporte o servicios de mensajería confiables. Se debe acordar con la gerencia una lista de servicios de mensajería autorizados e implementar un procedimiento para verificar la identificación de los mismos.
b) El embalaje debe ser suficiente como para proteger el contenido contra eventuales daños físicos durante el tránsito y debe seguir las especificaciones de los fabricantes o proveedores.
c) Se deben adoptar controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen
    1) uso de recipientes cerrados;
    2) entrega en mano;
    3) embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso);
    4) en casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

8.7.3 Seguridad del comercio electrónico

El comercio electrónico puede comprender el uso de intercambio electrónico de datos (EDI), correo electrónico y transacciones en línea a través de redes públicas como Internet. El comercio electrónico es vulnerable a diversas amenazas relativas a redes, que pueden tener como resultado actividades fraudulentas, disputas contractuales y divulgación o modificación de información. Se deben aplicar controles para proteger al comercio electrónico de dichas amenazas. Las consideraciones en materia de seguridad con respecto al comercio electrónico deben incluir las siguientes:

a) Autenticación. Qué nivel de confianza recíproca deben requerir el cliente y comerciante con respecto a la identidad alegada por cada uno de ellos?
b) Autorización. Quién está autorizado a fijar precios, emitir o firmar los documentos comerciales clave? Cómo conoce este punto el otro participante de la transacción.
c) Procesos de oferta y contratación. Cuáles son los requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos?
d) Información sobre fijación de precios. Qué nivel de confianza puede depositarse en la integridad del listado de precios publicado y en la confidencialidad de los acuerdos relativas a descuentos?
e) Transacciones de compra. Cómo es la confidencialidad e integridad de los datos suministrados con respecto a órdenes, pagos y direcciones de entrega, y confirmación de recepción?
f) Verificación. Qué grado de verificación es apropiado para constatar la información de pago suministrada por el cliente?

g) Cierre de la transacción. Cuál es forma de pago más adecuada para evitar fraudes?
h) Ordenes. Qué protección se requiere para mantener la confidencialidad e integridad de la información sobre órdenes de compra y para evitar la pérdida o duplicación de transacciones.
i) Responsabilidad. Quién asume el riesgo de eventuales transacciones fraudulenta

Gran parte de las consideraciones mencionadas pueden resolverse mediante la aplicación de las técnicas criptográficas enumeradas en el punto 10.3, tomando en cuenta el cumplimiento de los requisitos legales (ver 12.1, en particular los puntos 12.1.6 para legislación sobre criptografía).

Los acuerdos de comercio electrónico entre partes, deben ser respaldados por un acuerdo documentado que comprometa a las mismas a respetar los términos y condiciones acordados, incluyendo los detalles de autorización [ver el punto b), más arriba]. Pueden requerirse otros acuerdos con proveedores de servicios de información y de redes que aporten beneficios adicionales.

Los sistemas públicos de transacciones deben dar a conocer a sus clientes sus términos y condiciones comerciales.

Se debe tomar en cuenta la resistencia a ataques con que cuenta el "host" utilizado para el comercio electrónico, y las implicancias de seguridad de las interconexiones de red que se requieren para su implementación (ver 9.4.7).

8.7.4 Seguridad del correo electrónico

8.7.4.1 Riesgos de seguridad

El correo electrónico se está utilizando para las comunicaciones comerciales, en reemplazo de las formas tradicionales de comunicación como el telex y el correo postal. El correo electrónico difiere de las formas tradicionales de comunicaciones comerciales por su velocidad, estructura de mensajes, grado de informalidad y vulnerabilidad a las acciones no autorizadas. Se debe tener en cuenta la necesidad de controles para reducir los riesgos de seguridad creados por el correo electrónico. Los riesgos relativos a la seguridad comprenden :

a) vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio
b) vulnerabilidad a errores, por ej., consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio ;
c) impacto de un cambio en el medio de comunicación en los procesos de negocio, por ej., el efecto del incremento en la velocidad de envío o el efecto de enviar mensajes formales de persona a persona en lugar de mensajes entre organizaciones
d) consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación
e) implicancias de la publicación externa de listados de personal, accesibles al público ;
f) control del acceso de usuarios remotos a las cuentas de correo electrónico.

8.7.4.2 Política de correo electrónico

Las organizaciones deben elaborar una política clara con respecto al uso del correo electrónico, que incluya los siguientes tópicos:

a) ataques al correo electrónico, por ej. virus, interceptación
b) protección de archivos adjuntos de correo electrónico;
c) lineamientos sobre cuando no utilizar correo electrónico;

d) responsabilidad del empleado de no comprometer a la organización, por ej. enviando correos electrónicos difamatorios, llevando a cabo prácticas de hostigamiento, o realizando compras no autorizadas;
e) uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (ver 10.3)
f) retención de mensajes que, si se almacenaran, podrían ser hallados en caso de litigio;
g) controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

8.7.5 Seguridad de los sistemas electrónicos de oficina

Se deben preparar e implementar políticas y lineamientos para controlar las actividades de la empresa y riesgos de seguridad relacionados con los sistemas electrónicos de oficina. Éstos propician la difusión y distribución más rápidas de la información de la empresa mediante una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales y máquinas de fax.

Las consideraciones respecto de las implicancias de seguridad y comerciales al interconectar tales servicios, deben incluir:

a) vulnerabilidades de la información en los sistemas de oficina, por ej. la grabación de llamadas telefónicas o tele conferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo;
b) política y controles apropiados para administrar la distribución de información, por ej. el uso de boletines electrónicos corporativos (ver 9.1)
c) exclusión de categorías de información sensible de la empresa, si el sistema no brinda un adecuado nivel de protección (ver 5.2)
d) limitación del acceso a la información de agenda de personas determinadas, por ej. el personal que trabaja en proyectos sensibles ;
e) la aptitud del sistema para dar soporte a las aplicaciones de la empresa, como la comunicación de órdenes o autorizaciones
f) categorías de personal, contratistas o socios a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo (ver 4.2);
g) restricción de determinadas instalaciones a específicas categorías de usuarios;
h) identificación de la posición o categoría de los usuarios, por ej. empleados de la organización o contratistas en directorios a beneficio de otros usuarios ;
i) retención y resguardo de la información almacenada en el sistema (ver 12.1.3 y 8.4.1)
j) requerimientos y disposiciones relativos a sistemas de soporte UPC de reposición de información perdida (ver 1 1.1).

8.7.6 Sistemas de acceso público

Se deben tomar recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la organización que emite la publicación. Es posible que la información de un sistema de acceso público, por ej. la información en un servidor Web accesible por Internet, deba cumplir con leyes, normas y estatutos de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción. Debe existir un proceso de autorización formal antes de que la información se ponga a disposición del público.

El software, los datos y demás información que requiera un alto nivel de integridad, y que esté disponible en un sistema de acceso público, deben ser protegidos, mediante mecanismos adecuados, por ej. firmas digitales (ver 10.3.3). Los sistemas de publicación electrónica, en particular aquellos que

permiten "feedback" e ingreso directo de información, deben ser cuidadosamente controlados de manera que:

a) la información se obtenga de acuerdo con la legislación de protección de datos (ver 12.1.4);
b) la información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna;
c) la información sensible sea protegida durante el proceso de recolección y durante su almacenamiento;
d) el acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

8.7.7 Otras formas de intercambio de información

Se deben implementar procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo. La información puede verse comprometida debido a la falta de concientización, políticas o procedimientos acerca del uso de dichos medios, por ej. al escucharse una conversación por teléfono móvil en un lugar público, al escucharse los mensajes grabados en un contestador automático, mediante el acceso no autorizado a sistemas de correo de voz por discado, o al enviar accidentalmente faxes a la persona equivocada.

Si los servicios de comunicaciones fallan, se sobrecargan o se interrumpen, las operaciones de la empresa podrían verse interrumpidas y la información comprometerse (ver puntos 7.2 y 1 l). La información también podría comprometerse si usuarios no autorizados acceden a estos servicios (ver punto 9).

Se debe establecer una política clara con respecto a los procedimientos que deberá seguir el personal al establecer comunicaciones de voz, fax y vídeo. Esta debe incluir lo siguiente:

a) recordar al personal que debe tomar las debidas precauciones, por ej. no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:
    1) personas cercanas, en especial al utilizar teléfonos móviles;
    2) intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias (“scanners”) al utilizar teléfonos móviles análogos;
    3) personas en el lado receptor;
b) recordar al personal que no debe sostener conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas;
c) no dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado
d) recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:
    1) el acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos;
    2) la programación deliberada o accidental de equipos para enviar mensajes a determinados números ;
    3) el envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

9 CONTROL DE ACCESOS

9.1 Requerimientos de negocio para el control de accesos

Objetivo: Controlar el acceso de información.
El acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos la seguridad y de los negocios.
Para esta se deben tener en cuenta las políticas de difusión y autorización de la información:

9.1.1 Política de control de accesos

9.1.1.1 Requerimientos políticos y de negocios.

Se deben definir y documentar los requerimientos de negocio para el control de accesos. Las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, deben ser claramente establecidos en una declaración de política de accesos. Se debe otorgar a los usuarios y proveedores de servicio una clara enunciación de los requerimientos comerciales que deberán satisfacer los controles de acceso.

La política debe contemplar lo siguiente:

a) requerimientos de seguridad de cada una de las aplicaciones comerciales;
b) identificación de toda información relacionada con las aplicaciones comerciales;
c) las políticas de divulgación y autorización de información, por ej., el principio de necesidad de conocer, y los niveles de seguridad y la clasificación de la información;
d) coherencia entre las políticas de control de acceso y de clasificación de información de los diferentes sistemas y redes ;
e) legislación aplicable y obligaciones contractuales con respecto a la protección del acceso a datos y servicios (ver punto 12) ;
f) perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo ;
g) administración de derechos de acceso en un ambiente distribuido y de red que reconozcan todos los tipos de conexiones disponibles.

9.1.1.2 Reglas de control de accesos

Al especificar las reglas de control de acceso, se debe considerar cuidadosamente lo siguiente:

a) diferenciar entre reglas que siempre deben imponerse y reglas optativas o condicionales;
b) establecer reglas sobre la base de la premisa “Qué debe estar generalmente prohibido a menos que se permita expresamente?”, antes que la regla mas débil “Todo esta generalmente permitido a menos que se prohíba expresamente” ;
c) los cambios en los rótulos de información (ver 5.2) que son iniciados automáticamente por las instalaciones de procesamiento de información y aquellos el usuario inicia según su criterio;
d) los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que inicia el administrador;
e) las reglas que requieren la aprobación del administrador o de otros antes de entrar en vigencia y aquellas que no.

9.2 Administración de accesos de usuarios

Objeto: Impedir el acceso no autorizado en los sistemas de información.
Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.
Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema.

9.2.1 Registración de usuarios

Debe existir un procedimiento formal de registración y desregistración de usuarios para otorgar acceso a todos los sistemas y servicios de información multi-usuario. El acceso a servicios de información multi-usuario debe ser controlado a través de un proceso formal de registración de usuarios, el cual debe incluir los siguientes puntos:

a) utilizar IDs de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar ;
b) verificar que el usuario tiene autorización del propietario del sistema para el uso del sistema o servicio de información. También puede resultar apropiada una aprobación adicional de derechos de acceso por parte de la gerencia;
c) verificar que el nivel de acceso otorgado es adecuado para el propósito del negocios (ver 9.1) y es coherente con la política de seguridad de la organización, por ej. que no compromete la separación de tareas (ver 8.1.4) ;
d) entregar a los usuarios un detalle escrito de sus derechos de acceso;
e) requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso ;
f) garantizar que los proveedores de servicios no otorgan acceso hasta que se hayan completado los procedimientos de autorización ;
g) mantener un registro formal de todas las personas registradas para utilizar el servicio ;
h) cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización ;
i) verificar periódicamente, y cancelar IDs y cuentas de usuarios redundantes;
j) garantizar que los IDs de usuario redundantes no se asignen a otros usuarios;

Se debe considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados (ver también 6.1.4. y 6.3.5.)

9.2.2 Administración de privilegios

Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente en el más importante factor que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Deben identificarse los privilegios asociados a cada producto del sistema por ej. sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento, por ej. el requerimiento mínimo para su rol funcional solo cuando sea necesario.
c) Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.
d) Se debe promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
e) Los privilegios deben asignarse a una identidad de usuario diferente de aquellas utilizadas en los actividades comerciales normales.

9.2.3 Administración de contraseñas de usuario

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de administración formal, mediante el cual debe llevarse a cabo lo siguiente:

a) requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo (esto podría incluirse en los términos y condiciones de empleo, ver 6.1.4);
b) garantizar, cuando se requiera que los usuarios mantengan a sus propias contraseñas, que se provea inicialmente a los mismos de una contraseña provisoria segura, que deberán cambiar de inmediato. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, solo debe suministrarse una vez identificado el usuario;
c) requerir contraseñas provisorias para otorgar a los usuarios de manera segura. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro). Los usuarios deben acusar recibo de la recepción de la clave (password);

Las contraseñas nunca deben ser almacenadas en sistemas informativos sin protección (ver 9.5.4).

Se resulta pertinente, se debe considerar el uso de otras tecnologías de identificación y autenticación de usuarios, como la biométrica, por Ej... verificación de huellas dactilares, verificación de firma y uso de “tokens” de hardware, como las tarjetas de circuito integrado (“chip-cards”).

9.2.4 Revisión de derechos de acceso de usuario

A fin de mantener un control eficaz del acceso a los datos y servicios de información, la gerencia debe llevar a cabo un proceso formal a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios, de manera tal que:

a) los derechos de acceso de los usuarios se revisen a intervalos regulares (se recomienda un periodo de seis meses) y después de cualquier cambio (ver 9.2.1);
b) las autorizaciones de privilegios especiales de derechos de acceso (ver 9.2.2) se revisen a intervalos mas frecuentes (se recomienda un periodo de tres meses) ;
c) las asignaciones de privilegios se verifiquen a intervalos regulares, a fin de garantizar que no se obtengan privilegios no autorizados.

9.3 Responsabilidades del usuario

Objeto: Impedir el acceso usuarios no autorizados La cooperación de los usuarios autorizados en esencial para la eficacia de la seguridad. Se debe concienciar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

9.3.1 Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
Las contraseñas constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:

a) mantener las contraseñas en secreto;
b) evitar mantener un registro en papel de las contraseñas, a menos que este pueda ser almacenado en forma segura;
c) cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas;
d) seleccionar contraseñas de calidad, con una longitud mínima de seis caracteres que:
    1) sean fácil de recordar;
    2) no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ej. nombres, números de teléfono, fecha de nacimiento, etc. ;
    3) no tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
e) cambiar las contraseñas a intervalos regulares o según el número de acceso (las contraseñas de cuentas con privilegios deben ser modificadas con mayor frecuencia que las contraseñas comunes), y evitar reutilizar o reciclar viejas contraseñas ;
f) cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”) ;
g) no incluir contraseñas en los procesos automatizados de inicio de sesión, por ej. aquellas almacenadas en una tecla de función o macro ;
h) no compartir las contraseñas individuales de usuario.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se debe notificar a los mismos que pueden utilizar una contraseña de calidad única (ver 9.3.1) para todos los servicios que brinden un nivel razonable de protección de las contraseñas almacenadas.

9.3.2 Equipos desatendidos en áreas de usuarios

Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ej. estaciones de trabajo o servidores de archivos, pueden requerir una protección específica contra accesos no autorizados, cuando se encuentran desatendidos durante un periodo extenso. Se debe concientizar a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección.

Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:

a) concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ej. un preservador de pantallas protegido por contraseña ;
b) llevar a cabo el procedimiento de salida de los procesadores centrales cuando finaliza la sesión (no solo apagar la PC o terminal) ;
c) proteger las PCs o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ej. contraseña de acceso, cuando no se utilizan.

9.4 Control de acceso a la red

Objetivo: La protección de los servicios de red.
Se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios, garantizando:

a) interfaces inadecuadas entre la red de la organización y las redes de otras organizaciones, o redes publicas ;
b) mecanismos de autenticación apropiados para usuarios y equipamiento ;
c) control de acceso de usuarios a los servicios de información.

9.4.1 Política de utilización de los servicios de red

Las conexiones no seguras a los servicios de red pueden afectar a toda la organización. Los usuarios solo deben contar con acceso directo a los servicios para los cuales han sido expresamente autorizados. Este control es particularmente importante para las conexiones de red a aplicaciones comerciales sensibles o críticas o a usuarios en sitios de alto riesgo, por ej. áreas públicas o externas que están fuera de la administración y el control de seguridad de la organización.

Se debe formular una política concerniente al uso de redes y servicios de red. Esta debe comprender:

a) las redes y servicios de red a los cuales se permite el acceso ;
b) procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales tienen permitido el acceso ;
c) controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta política debe ser coherente con la política de control de accesos de la organización (ver 9.1).

9.4.2 Camino forzado

Puede resultar necesario controlar el camino desde la terminal de usuario hasta el servicio informático. Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad de ruteo. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de negocios, o para el uso no autorizado de servicios de información. Estos riesgos pueden reducirse mediante la incorporación de controles, que limiten la ruta entre una terminal de usuario y los servicios del computador, a los cuales sus usuarios están autorizados a acceder, por ej. creando un camino forzado.

El objetivo de un camino forzado es evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo esta autorizado a acceder.

Esto normalmente requiere la implementación de varios controles en diferentes puntos de la ruta. El principio es limitar las opciones de ruteo en cada punto de la red, a través de elecciones predefinidas.

A continuación se enumeran los ejemplos pertinentes:

a) asignación de números telefónicos o líneas dedicadas ;
b) conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos;
c) limitar las opciones de menú y submenú de cada uno de los usuarios ;
d) evitar la navegación ilimitada por la red ;
e) imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red ;
f) controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ej, firewalls;
g) restringir el acceso a redes, estableciendo dominios lógicos separados, por ej., redes privadas virtuales para grupos de usuarios dentro de la organización (ver también 9.4.6);

Los requerimientos relativos a enrutamientos forzados deben basarse en la política de control de accesos de la organización. (9.1).

9.4.3 Autenticación de usuarios para conexiones externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la empresa, por ej., accesos mediante discado. Por consiguiente, el acceso de usuarios remotos debe estar sujeto a la autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros, por ej. los métodos basados en el uso de técnicas criptográficas pueden proveer de una fuerte autenticación. Es importante determinar mediante una evaluación de riesgos el nivel de protección requerido. Esto es necesario para la adecuada selección del método.

La autenticación de usuarios remotos puede llevarse a cabo utilizando, por ejemplo, una técnica basada en criptografía, “tokens” de hardware, o un protocolo de pregunta/respuesta. También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de rellamada o dail-back, por ej. utilizando módems de dial-back, pueden brindar protección contra conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información de la organización. Este tipo de control autentica a los usuarios que intentan establecer una conexión con una red de la organización desde locaciones remotas. Al aplicar este control, la organización no debe utilizar servicios de red que incluyan desvío de llamadas o, si lo hacen, deben inhabilitar el uso de dichas herramientas para evitar las debilidades asociadas con la misma. Asimismo, es importante que el proceso de rellamada garantice que se produzca una desconexión real del lado de la organización. De otro modo, el usuario remoto podría mantener la línea abierta fingiendo que se ha llevado a cabo la verificación de rellamada. Los procedimientos y controles de rellamada deben ser probados exhaustivamente respecto de esta posibilidad.

9.4.4 Autenticación de nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la empresa. Por consiguiente, las conexiones a sistemas informativos remotos deben ser autenticadas. Esto es particularmente importante si la conexión utiliza una red que esta fuera de control de la gestión de seguridad de la organización. En el punto 9.4.3 se enumeran algunos ejemplos de autenticación y de cómo pude lograrse. La autentica-

ción de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido (ver 9.4.3).

9.4.5 Protección de los puertos (ports) de diagnostico remoto

El acceso a los puertos de diagnostico debe ser controlado de manera segura. Muchas computadoras y sistemas de comunicación son instalados con una herramienta de diagnostico remoto por discado, para uso de los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnostico proporcionan un medio de acceso no autorizado. Por consiguiente, deben ser protegidos por un mecanismo de seguridad apropiado, por ej. una cerradura de seguridad y un procedimiento que garantice que solo son accesibles mediante un acuerdo entre el gerente de servicios informativos y el personal de soporte de hardware y software que requiere acceso.

9.4.6 Subdivisión de redes

Las redes se están extendiendo en forma creciente mas allá de los limites tradicionales de la organización, a medida que se constituyen sociedades con requerimientos de interconexión, o uso compartido de instalaciones de procesamiento de información y redes. Dichas extensiones pueden incrementar el riesgo de acceso no autorizado a sistemas de información ya existentes que utilizan la red, algunos de los cuales podrían requerir de protección contra otros usuarios de red, debido a su sensibilidad o criticidad. En tales circunstancias, se debe considerar la introducción de controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

Un método para controlar la seguridad de redes extensas es dividirlas en dominios lógicos separados, por ej. dominios de red internos y externos de una organización, cada uno protegido por un perímetro de seguridad definido. Dicho perímetro puede ser implementado mediante la instalación de una compuerta (“gateway”) segura entre las dos redes que han de ser interconectadas, para controlar el acceso y flujo de información entre los dos dominios. Este “gateway” debe ser configurado para filtrar el tráfico entre los dominios (ver 9.4.7 y 9.4.8) y para bloquear el acceso no autorizado de acuerdo con la política de control de accesos de la organización (ver 9.1). Un ejemplo de este tipo de “gateway” es lo que comúnmente se conoce como “firewall”.

Los criterios para la subdivisión de redes en dominios deben basarse en la política de control de accesos y los requerimientos de acceso (ver 9.1), y también tomar en cuenta el costo relativo y el impacto del desempeño que ocasiona la incorporación de un enrutador de red o una tecnología de “gateways” adecuados (ver 9.4.7 y 9.4.8).

9.4.7 Control de conexión a la red

Los requerimientos de la política de control de accesos para redes compartidas, especialmente aquellas que se extiendan mas allá de los limites de la organización, pueden requerir la incorporación de controles para limitar la capacidad de conexión de los usuarios. Dichos controles pueden implementarse mediante “gateways” de red que filtren el tráfico por medio de reglas o tablas previamente definidas. Las restricciones aplicadas deben basarse en la política y los requerimientos de acceso de las aplicaciones de la empresa (ver 9.1), y deben mantenerse y actualizarse de conformidad.

A continuación se enumeran ejemplos de aplicaciones a las cuales deben aplicarse restricciones:

a) correo electrónico ;
b) transferencia unidireccional de archivos ;
c) transferencia de archivos en ambas direcciones ;
d) acceso interactivo ;
e) acceso de red vinculado a hora o fecha.

9.4.8 Control de ruteo de red

Las redes compartidas, especialmente aquellas que se extienden mas allá de los limites organizacionales, pueden requerir la incorporación de controles de ruteo para garantizar que las conexiones informáticas y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales (ver 9.1). Este control es a menudo esencial para las redes compartidas con usuarios externos (no organizadores).

Los controles de ruteo deben basarse en la verificación positiva de direcciones de origen y destino.

La traducción de direcciones de red también constituye un mecanismo muy útil para aislar redes y evitar que las rutas se propaguen desde la red de una organización a la red de otra. Pueden implementarse en software o hardware. Quienes lleven a cabo la implementación deben estar al corriente de la fortaleza de los mecanismos utilizados.

9.4.9 Seguridad de los servicios de red

Existe una amplia gama de servicios de red privados o públicos, algunos de los cuales ofrecen servicios con valor agregado. Los servicios de red pueden tener características de seguridad únicas o complejas. Las organizaciones que utilizan servicios de red deben garantizar que se provea de una clara descripción de los atributos de seguridad de todos los servicios utilizados.

9.5 Control de acceso al sistema operativo

Objetivo: Impedir el acceso no autorizado al computador

Los mecanismos de seguridad a nivel del sistema operativo deben ser utilizados para restringir el acceso a los recursos del computador. Estas facilidades deben tener la capacidad de llevar a cabo lo siguiente:

a) identificar y verificar la identidad y, si fuera necesario, la terminal o ubicación de cada usuario autorizado ;
b) registrar los accesos exitosos y fallidos al sistema ;
c) suministrar medios de autenticación apropiados; si se utiliza un sistema de administración de contraseñas, éste debe asegurar la calidad de las mismas (ver 9.3.1 d) ;
d) restringir los tiempos de conexión de los usuarios, según corresponda

Se debe disponer de otros métodos de control de acceso, como “challenge-response”, si están justificados por el riesgo comercial..

9.5.1 Identificación automática de terminales

Se debe tener en cuenta la identificación automática de terminales para autenticar conexiones a ubicaciones específicas y a equipamiento portable. La identificación automática de terminales es una técnica que puede utilizarse si resulta importante que la sesión solo pueda iniciarse desde una terminal informática o una ubicación determinadas. Puede utilizarse un identificador en la terminal, o adjunto a la misma, para indicar si esta terminal especifica esta autorizada a iniciar o recibir ciertas transacciones. Puede resultar necesario aplicar protección física a la terminal, a fin de mantener la seguridad del identificador de la misma. También pueden utilizarse otras técnicas para autenticar usuarios (ver 9.4.3).

9.5.2 Procedimientos de conexión de terminales

El acceso a los servicios de información debe ser posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático debe ser diseñado para minimizar la oportunidad

de acceso no autorizado. Este procedimiento, por lo tanto debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de identificación debería:

a) no desplegar identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión;
b) desplegar un aviso general advirtiendo que solo los usuarios autorizados pueden acceder a la computadora ;
c) no dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión ;
d) validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta ;
e) limitar el número de intentos de conexión no exitosos permitidos (se recomiendan tres) y considerar:
    1) registrar los intentos no exitosos ;
    2) implementar una demora obligatoria antes de permitir otros intentos de identificación, o rechazar otros intentos sin autorización especifica ;
    3) desconectar conexiones de data link ;
f) limitar el tiempo máximo y mínimo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión ;
g) desplegar la siguiente información al completarse una conexión exitosa:
    1) flechas y hora de la conexión exitosa anterior;
    2) detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

9.5.3 Identificación y autenticación de los usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los IDs de usuario no deben dar ningún inicio del nivel de privilegio del usuario (ver 9.2.2), por ej. gerente, supervisor, etc.

En circunstancias excepcionales, cuando existe un claro beneficio para la empresa, pueda utilizarse un ID compartido para un grupo de usuarios o una tarea especifica. Para casos de esta índole, se debe documentar la aprobación de la gerencia. Podrían requerirse controles adicionales para mantener la responsabilidad.

Existen diversos procedimientos de autenticación, los cuales pueden ser utilizados para sustentar la identidad alegada del usuario. Las contraseñas (ver también 9.3.1 y más abajo) constituyen un medio muy común para proveer la identificación y autenticación (I y A) sobre la base de un secreto que solo conoce el usuario. También se puede llevar a cabo lo mismo con medios criptográficos y protocolos de autenticación.

Los objetos como “tokens” con memoria o tarjetas inteligentes que poseen los usuarios también pueden utilizarse para I y A. Las tecnologías de autenticación biométrica que utilizan las características o atributos únicos de un individuo también pueden utilizarse para autenticar la identidad de una persona. Una combinación de tecnologías y mecanismos vinculados de manera segura tendrá como resultado una autenticación más fuerte.

9.5.4 Sistema de administración de contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad (ver 9.3.1 como orientación acerca del uso de contraseñas).

Algunas aplicaciones requieren que las contraseñas de usuario sean asignadas por una autoridad independiente. En la mayoría de los casos las contraseñas son seleccionadas y mantenidas por los usuarios.

Un buen sistema de administración de contraseñas debe:

a) imponer el uso de contraseñas individuales para determinar responsabilidades;
b) cuando corresponda, permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso;
c) imponer una selección de contraseñas de calidad según lo señalado en el punto 9.3.1 ;
d) cuando los usuarios mantienen sus propias contraseñas, imponer cambios en las mismas según lo señalado en el punto 9.3.1 ;
e) cuando los usuarios seleccionan contraseñas, obligarlos a cambiar las contraseñas temporarias en su primer procedimiento de identificación (ver 9.2.3) ;
f) mantener un registro de las contraseñas previas del usuario, por ej. de los 12 meses anteriores, y evitar la reutilización de las mismas ;
g) no mostrar las contraseñas en pantalla, cuando son ingresadas ;
h) almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación;
i) almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional ;
j) modificar las contraseñas predeterminadas por el vendedor, una vez instalado el software.

9.5.5 Uso de utilitarios de sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) uso de procedimientos de autenticación para utilitarios del sistema ;
b) separación entre utilitarios del sistema y software de aplicaciones ;
c) limitación de uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados ;
d) autorización para uso ad hoc de utilitarios de sistema ;
e) limitación de la disponibilidad de utilitarios de sistema, por ej. a la duración de un cambio autorizado ;
f) registro de todo uso de utilitarios del sistema ;
g) definición y documentación de los niveles de autorización para utilitarios del sistema ;
h) remoción de todo el software basado en utilitarios y software de sistema innecesarios.

9.5.6 Alarmas silenciosas para la protección de los usuarios

Debe considerarse la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrarse una alarma de esta índole debe basarse en una evaluación de riesgos. Se deben definir responsabilidades y procedimientos para responder a la activación de una alarma silenciosa.

9.5.7 Desconexión de terminales por tiempo muerto

Las terminales inactivas en ubicaciones de alto riego, por ej. áreas públicas o externas fuera del alcance de la gestión de seguridad de la organización, o que sirven a sistemas de alto riego, deben apagarse después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto debe limpiar la pantalla de la terminal y debe cerrar tanto la sesión de la aplicación como la de red, después de un periodo definido de inactividad. El lapso por tiempo muerto debe responder a los riesgos de seguridad del área y de los usuarios de la terminal.

Para algunas PCs, puede suministrarse una herramienta limitada de desconexión de terminal por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

9.5.8 Limitación del horario de conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminal a los servicios informativos reduce el espectro de oportunidades para el acceso no autorizado. Se debe considerar un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ej. áreas publicas o externas que estén fuera del alcance de la gestión de seguridad de la organización. Entre los ejemplos de dichas restricciones se pueden enumerar los siguientes:

a) utilización de lapsos predeterminados, por ej. para transmisiones de archivos e lote, o sesiones interactivas periódicas de corta duración ;
b) limitación de los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria..

9.6 Control de acceso a las aplicaciones

Objetivo: Impedir el acceso no autorizado a la información contenida en los sistemas de información.
Las herramientas de seguridad deben ser utilizadas para limitar el acceso no dentro de los sistemas de aplicación.
El acceso lógico al software y a la información debe estar limitado a los usuarios autorizados. Los sistemas de aplicación deben:

a) controlar el acceso de usuarios a la información y a las funciones de los sistemas de aplicación, de acuerdo con la política de control de accesos definida por la organización ;
b) brindar protección contra el acceso no autorizado de utilitarios y software del sistema operativo que tengan la capacidad de pasar por alto los controles de sistemas o aplicaciones ;
c) no comprometer la seguridad de otros sistemas con los que se comparten recursos de información ;
d) tener la capacidad de otorgar acceso a la información únicamente al propietario, a otros individuos autorizados mediante designación formal, o a grupos de definidos de usuarios.

9.6.1 Restricción del acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, deben tener acceso a la información y a las funciones de los sistemas de aplicación de conformidad con una política de control de acceso definida, sobre la base de los requerimientos de cada aplicación comercial, y conforme a la

política de la organización para el acceso a la información, (ver 9.1). se debe considerar la aplicación de los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) provisión de menús para controlar el acceso a las funciones de los sistemas de aplicación ;
b) restricción del conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizadas a acceder, con la adecuada edición de documentación de usuario ;
c) control de los derechos de acceso de los usuarios, por ej. lectura, escritura, supresión y ejecución ;
d) garantizar que las salidas (outputs) de los sistemas de aplicación que administran información sensible, contengan solo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas, y revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

9.6.2 Aislamiento de sistemas sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a perdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) La sensibilidad de un sistema de aplicación debe ser claramente identificada y documentada por el propietario de la aplicación (ver 4.1.3)
b) Cuando una aplicación sensible ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales esta compartirá los recursos deben ser identificados y acordados con el propietario de la aplicación sensible.

9.7 Monitoreo del acceso y uso de los sistemas

Objetivo: detectar actividades no autorizadas Los sistemas deben ser monitoreados para detectar desviaciones respecto de la política de control de accesos y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad. El monitoreo de los sistemas permite comprobar la eficacia de los controles adoptados y verificar la conformidad con el modelo de política de acceso (ver 9.1)

9.7.1 Registro de eventos

Deben generarse registros de auditoria que contengan excepciones y otros eventos relativos a seguridad, y deben mantenerse durante un periodo definido para acceder en futuras investigaciones y en el monitoreo de control de accesos. Los registros de auditorias también deben incluir:

a) ID de usuario;
b) Fecha y hora de inicio y terminación ;
c) Identidad o ubicación de la terminal, si es posible ;
d) Registros de intentos exitosos fallidos de acceso al sistema ;
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

Podría requerirse que ciertos registros de auditoria sean archivados como parte de la política de retención de registros o debido a los requerimientos de recolección de evidencia (ver también el punto 12).

9.7.2 Monitoreo del uso de los sistemas

9.7.2.1 Procedimientos y áreas de riesgo

Se debiera establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información. Dichos procedimientos son necesarios para garantizar que los usuarios solo estén desempeñando actividades que hayan sido autorizadas explícitamente. El nivel de monitoreo requerido para cada una las instalaciones debe determinarse mediante una evaluación de riesgos.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) acceso no autorizado, incluyendo detalles como:
    1) ID de usuario;
    2) Fecha y hora de eventos clave;
    3) Tipos de eventos;
    4) Archivos a los que se accede;
    5) Utilitarios y programas utilizados
b) todas las operaciones con privilegio, como:
    1) Utilización de cuenta de supervisor;
    2) Inicio y cierre (start-up and stop) del sistema;
    3) Conexión y desconexión de dispositivos I/O;
c) intentos de acceso no autorizado, como:
    1) Intentos fallidos;
    2) Violaciones de la política de accesos y notificaciones para “gateways” de red y “firewalls”;
    3) Alertas de sistemas patentados para detención de intrusiones ;
d) alertas o fallas de sistema como:
    1) alertas o mensajes de consola ;
    2) excepciones del sistema de registro;
    3) alarmas del sistema de administración de redes.

9.7.2.2 Factores de riesgo

Se debe revisar periódicamente el resultado de las actividades de monitoreo. La frecuencia de la revisión debe depender de los riesgos involucrados. Entre los factores de riesgo que se deben considerar se encuentran:

a) la criticidad de los procesos de aplicaciones ;
b) el valor, la sensibilidad o criticidad de la información involucrada ;
c) la experiencia acumulada en materia de infiltración y uso inadecuado del sistema ;
d) el alcance de la interconexión del sistema (en particular las redes publicas)

9.7.2.3 Registro y revisión de eventos

Una revisión de los registros implica la comprensión de las amenazas que afronta el sistema y las maneras que surgen. En el punto 9.7.1 se enumeran ejemplos de eventos que podrían requerir investigación adicional en caso de producirse incidentes relativos a la seguridad.

Frecuentemente, los registros del sistema contienen un gran volumen de información, gran parte de la cual es ajena al monitoreo de seguridad. Para asistir en la identificación de eventos significativos, a fin de desempeñar el monitoreo de seguridad, se debe considerar la posibilidad de copiar automáticamente los tipos de mensajes adecuados a un segundo registro, y/o utilizar herramientas de auditoria o utilitarios adecuados para llevar a cabo el examen de archivo.

Al asignar la responsabilidad por la revisión de registros, se debe considerar una separación de funciones entre quien/es emprende/n la revisión y aquellos cuyas actividades están siendo monitoreadas.

Se debe prestar especial atención a la seguridad de la herramienta de registro, debido a que si se accede a la misma en forma no autorizada, esto puede propiciar una falsa percepción de la seguridad. Los controles deben apuntar a proteger contra cambios no autorizados y problemas operativos. Estos incluyen:

a) la desactivación de la herramienta de registro ;
b) alteraciones a los tipos de mensajes registrados ;
c) archivos de registro editados o suprimidos ;
d) medio de soporte archivos de registro saturado, y falla en el registro de eventos o sobre escritura de los mismos.

9.7.3 Sincronización de relojes

La correcta configuración de los relojes de las computadoras es importante para garantizar la exactitud de los registros de auditoria, que pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios. Los registros de auditorias inexactos podrían entorpecer tales investigaciones y dañar la credibilidad de la evidencia.

Cuando una computadora o dispositivo de comunicaciones tiene la capacidad de operar un reloj en tiempo real, este se debe configurar según un estándar acordado, por ej. Tiempo Coordinado Universal (UCT) o tiempo estándar local. Como se sabe que algunos relojes se desajustan con el tiempo, debe existir un procedimiento que verifique y corrija cualquier variación significativa.

9.8 Computación móvil y trabajo remoto

Objetivo: Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remotas.
La protección requerida debe ser proporcional a los riesgos que originan estas formas especificas de trabajo. Cuando se utiliza computación móvil deben tenerse en cuenta los riesgos que implica trabajar en un ambiente sin protección y se debe implementar la protección adecuada. En el caso del trabajo remoto la organización debe implementar la protección en el sitio de trabajo remoto (“teleworking site”) y garantizar que se tomen las medidas adecuadas para este tipo de trabajo.

9.8.1 Computación móvil

Cuando se utilizan dispositivos informáticas móviles, por ej. notebooks, palmtops, laptops y teléfonos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información de la empresa. Se debe adoptar una política formal que tome en cuenta los riesgos que implica trabajar con herramientas informáticas móviles, en particular en ambientes no protegidos. Por ejemplo, dicha política debe incluir los requerimientos de protección física, controles de acceso, técnicas criptográficas, resguardos y protección contra virus. Esta política también debe incluir reglas y asesoramiento en materia de conexión de dispositivos móviles a redes y orientación sobre uso de estos dispositivos en lugares públicos.

Se deben tomar recaudos al utilizar dispositivos informáticos móviles en lugares públicos, salas de reuniones y otras áreas no protegidas fuera de la sede de la organización. Se debe implementar protección para evitar el acceso no autorizado a la información almacenada y procesada por estas herramientas, o la divulgación de la misma, por ej. mediante técnicas criptográficas (ver 10.3).

Es importante que cuando dichos dispositivos, son utilizadas en lugares públicos se tomen recaudos para evitar el riesgo de que la información que aparece en pantalla, sea vista por personas no autorizadas. Se deben implementar procedimientos contra software malicioso y estos deben mantenerse actualizados (ver 8.3). El equipamiento debe estar disponible para permitir un procedimiento de resguardo de la información rápido y fácil.. Estos procedimientos deben estar adecuadamente protegidos contra, por ej., robo o pérdida de la información.

Se debe brindar protección adecuada para el uso de dispositivos móviles conectadas a redes. El acceso remoto a la información de la empresa a través de redes publicas, utilizando herramientas informáticas móviles, solo debe tener lugar después de una identificación y autenticación exitosas, y con mecanismos adecuados de control de acceso implementados (ver 9.4).
Los dispositivos informáticas móviles también deben estar físicamente protegidas contra robo, especialmente cuando se dejan, por ej. en automóviles y otros medios de transporte, habitaciones de hotel, centros de conferencias y ámbitos de reunión. El equipamiento que transporta información importante de la empresa, sensible y/o critica no debe dejarse desatendido y, cuando resulta posible, debe estar físicamente resguardado bajo llave, o deben utilizarse cerraduras especiales para asegurar el equipamiento. En el punto 7.2.5 se puede encontrar información adicional sobre la protección física del equipamiento móvil.

Se debe brindar entrenamiento al personal que utiliza computación móvil para incrementar su cocimiento de los riesgos adicionales ocasionados por esta forma de trabajo y de los controles que se deben implementar.

9.8.2 Trabajo remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar fijo fuera de la organización. Se debe implementar la protección adecuada del sitio de trabajo remoto contra, por ej. el robo de equipamiento e información, la divulgación no autorizada de información, el acceso remoto no autorizada a los sistemas internos de la organización o el uso inadecuado de los dispositivos e instalaciones. Es importante que el trabajo remoto sea autorizado y controlado por la gerencia, y que se implementen disposiciones y acuerdos para esta forma de trabajo.

Las organizaciones deben considerar el desarrollo de una política, de procedimientos y de estándares para controlar las actividades de trabajo remoto.

Las organizaciones sólo deben autorizar actividades de trabajo remoto si han comprobado satisfactoriamente que se han implementado disposiciones y controles adecuados en materia de seguridad y que estos cumplen con la política de seguridad de la organización. Se deben considerar los siguientes ítems:

a) la seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local;
b) el ambiente de trabajo remoto propuesto;
c) los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que pasará a través del vinculo de comunicación y la sensibilidad del sistema interno;
d) la amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ej. familia y amigos.

Los controles y disposiciones comprenden:

a) la provisión de mobiliario para almacenamiento y equipamiento, adecuado para las actividades de trabajo remoto;

b) una definición del trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar y los sistemas internos y servicio a los cuales el trabajador remoto esta autorizado a acceder;
c) la provisión de un adecuado equipamiento de comunicación, con inclusión de métodos para asegurar el acceso remoto;
d) seguridad física;
e) reglas y orientación para cuando familiares y visitantes accedan al equipamiento e información;
f) la provisión de hardware y el soporte y mantenimiento del software;
g) los procedimientos de back-up y para la continuidad de las operaciones;
h) auditoría y monitoreo de la seguridad;
i) anulación de la autoridad, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

10 DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

10.1 Requerimientos de seguridad de los sistemas.

Objetivo: Asegurar que la seguridad es incorporada a los sistemas de información.

Esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.
Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados como una parte de la totalidad del caso de negocios de un sistema de información.

10.1.1 Análisis y especificaciones de los requerimientos de seguridad.

Las comunicaciones de requerimientos comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben aplicar consideraciones similares al evaluar paquetes de software para aplicaciones comerciales. Si se considera adecuado, la administración puede querer utilizar productos certificados y evaluados en forma independiente.

Los requerimientos de seguridad y los controles deben reflejar el valor comercial de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.

Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

10.2 Seguridad en los sistemas de aplicación

Objetivo: Prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación.

Se deben diseñar en los sistemas de aplicación, incluyendo las aplicaciones realizadas por el usuario, controles apropiados y pistas de auditoria o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salida de datos.

Pueden ser necesarios controles adicionales para sistemas que procesan o tienen impacto en recursos sensitivos, valiosos o críticos de la organización. Tales controles deben ser determinados sobre la base de requerimientos de seguridad y evaluación de riesgo.

10.2.1 Validación de datos de entrada

Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados. Los controles deben ser aplicados a las entradas de las transacciones de negocios, datos permanentes (nombres y direcciones, límites de crédito, números de referencia al cliente) y tablas de parámetros (precios de venta, tasa de impuestos, índice de conversión de dinero). Se deben considerar los siguientes controles:

a) entrada dual u otros controles de entrada para detectar los siguientes errores:
    1) valores fuera de rango;
    2) caracteres inválidos en campos de datos;
    3) datos faltantes o incompletos;
    4) volúmenes de datos que exceden los limites inferior y superior;
    5) controles de datos no autorizados o inconsistentes;
b) revisión periódica de los contenidos de campos clave o archivos de datos para confirmar su validez e integridad;
c) inspección de los documentos de entrada para detectar cambios no autorizados en los datos de entrada (todos los cambios a los documentos de entrada deben ser autorizados);
d) procedimientos para responder a errores de validación;
e) procedimientos para determinar la verosimilitud de los datos;
f) determinación de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

10.2.2 Controles de procesamiento interno.

10.2.2.1 Áreas de riesgo.

Los datos que han sido correctamente ingresados pueden viciarse al procesar errores o a través de actos deliberados. Los controles de validación deben ser incorporados a los sistemas para detectar tal corrupción. El diseño de aplicaciones debe asegurar que las restricciones se implementen para minimizar los riesgos de fallas de procesamiento, conducentes a una pérdida de la integridad. Las áreas específicas a considerar incluyen:

a) el uso y localización dentro de los programas, de funciones de suma y borrado para realizar cambios en los datos;
b) los procedimientos para prevenir la ejecución de programas fuera de secuencia o cuando falló el procesamiento previo.
c) el uso de programas correctos para recuperación ante fallas, a fin de garantizar el procesamiento correcto de los datos.

10.2.2.2 Controles y verificaciones

Los controles requeridos dependerán de la naturaleza de la aplicación y del impacto de eventuales alteraciones de datos en el negocio. Entre los ejemplos de verificaciones que pueden ser incorporadas se encuentran los siguientes:

a) controles de sesión o de lote, para conciliar balances (saldos) de archivos de datos después de actualizaciones de transacciones;
b) controles de balance, para comparar balances de apertura con balances de cierre anteriores, por ejemplo:
    1. controles ejecución a ejecución;
    2. totales de actualización de archivos;
    3. controles programa a programa;
c) validación de datos generados por el sistema (ver 10.2.1);
d) verificaciones de la integridad de los datos o software bajados, o cargados, entre computadoras centrales y remotas (ver 10.3.3);
e) totales de control de registros y archivos;
f) verificaciones para garantizar que los programas de aplicación se ejecutan en el momento correcto;
g) comprobaciones para garantizar que los programas se ejecutan en el orden correcto y terminan en caso de producirse una falla, y que se detiene todo procesamiento posterior hasta que se resuelva el problema.

10.2.3 Autenticación de mensajes

La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados en el contenido de un mensaje transmitido electrónicamente, o para detectar alteraciones en el mismo.

Puede implementarse en hardware o software que soporte un dispositivo físico de autenticación de mensajes o un algoritmo de software.

Se debe tener en cuenta la autenticación de mensajes para aplicaciones en las cuales exista un requerimiento de seguridad para proteger la integridad del contenido del mensaje, por ej. transferencias electrónicas de fondos u otros intercambios electrónicos de datos similares. Se debe llevar a cabo una evaluación de riesgos de seguridad para determinar si se requiere una autenticación de mensajes y para identificar el método de implementación más adecuado.

La autenticación de mensajes no esta diseñada para proteger el contenido de un mensaje contra su divulgación no autorizada. Pueden utilizarse técnicas criptográficas (ver 10.3.2 y 10.3.3) como un medio adecuado de implementación de la autenticación de mensajes.

10.2.4 validación de los datos de salida

La salida de datos de un sistema de aplicación debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias. Normalmente, los sistemas se construyen suponiendo que si se ha llevado a cabo una validación, verificación y prueba apropiada, la salida siempre será correcta. Esto no siempre se cumple. La validación de salidas puede incluir:

a) comprobaciones de la razonabilidad para probar si los datos de salida son plausibles;
b) control de conciliación de cuentas para asegurar el procesamiento de todos los datos;
c) provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente, determine la exactitud, totalidad, precisión y clasificación de la información;
d) procedimientos para responder a las pruebas de validación de salidas;

e) definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

10.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información. Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

10.3.1 Política de utilización de controles criptográficos.

Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y conque propósito, y los procesos de la empresa.

Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto. Al desarrollar una política se debe considerar lo siguiente:

a) el enfoque gerencial respecto del uso de controles criptográficos en toda la organización, con inclusión de los principios generales según los cuales debe protegerse la información de la empresa;
b) el enfoque respecto de la administración de claves, con inclusión de los métodos para administrar la recuperación de la información cifrada en caso de perdida, compromiso o daño de las claves;
c) funciones y responsabilidades, por ej. quien es responsable de:
    1) la implementación de la política;
    2) la administración de las claves;
d) como se determinara el nivel apropiado de protección criptográfica;
e) los estándares que han de adoptarse para la eficaz implementación en toda la organización (que solución se aplica para cada uno de los procesos de negocio).

10.3.2 Cifrado

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debe tener en cuenta para la protección de información sensible o critica.

Mediante una evaluación de riesgos se debe identificar el nivel requerido de protección tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la política de la organización en materia criptográfica, se deben considerar las normas y restricciones nacionales que podrían aplicarse al uso de técnicas criptográficas, en diferentes partes del mundo, y las cuestiones relativas al flujo de información cifrada a través de las fronteras. Asimismo, se deben considerar los controles aplicables a la exportación e importación de tecnología criptográfica (ver también 12.1.6).

Se debe procurar asesoramiento especializado para identificar el nivel apropiado de protección, a fin de seleccionar productos adecuados que suministren la protección requerida, y la implementación de un sistema seguro de administración de claves (ver también 10.3.5). Asimismo, podría resultar necesario

obtener asesoramiento jurídico con respecto a las leyes y normas que podrían aplicarse al uso del cifrado que intenta realizar la organización.

10.3.3 Firma digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Por ejemplo, puede utilizarse en comercio electrónico donde existe la necesidad de verificar quien firma un documento electrónico y comprobar si el contenido del documento firmado ha sido modificado.

Las firmas digitales pueden aplicarse a cualquier tipo de documento que se procese electrónicamente, por ej., pueden utilizarse para firmar pagos, transferencias de fondos, contratos y convenios electrónicos. Pueden implementarse utilizando una técnica criptográfica sobre la base de un par de claves relacionadas de manera única, donde una clave se utiliza para crear una firma (la clave privada) y la otra, para verificarla (la clave publica).

Se den tomar recaudos para proteger la confidencialidad de la clave privada.

Esta clave debe mantenerse en secreto dado que una persona que tenga acceso a esta clave puede firmar documentos, por ej.: pagos y contratos, falsificando así la firma del propietario de la clave.

Asimismo, es importante proteger la integridad de la clave publica. Esta protección se provee mediante el uso de un certificado de clave publica (ver 10.3.5).

Es necesario considerar el tipo y la calidad del algoritmo de firma utilizado y la longitud de las claves a utilizar. Las claves criptográficas aplicadas a firmas digitales deben ser distintas de las que se utilizan para el cifrado (ver 10.3.2).

Al utilizar firmas digitales, se debe considerar la legislación pertinente que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación jurídica de las firmas digitales. Podría ser necesario establecer contratos de cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal es inadecuado. Se debe obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar la organización.

10.3.4 Servicios de No Repudio

Los servicios de no repudio deben utilizarse cuando es necesario resolver disputas acerca de la ocurrencia o no ocurrencia de un evento o acción, por ej. una disputa que involucre el uso de una firma digital en un contrato o pago electrónico. Pueden ayudar a sentar evidencia para probar que un evento o acción determinados han tenido lugar, por ej. cuando se objeta haber enviado una instrucción firmada digitalmente a través del correo electrónico. Estos servicios están basados en el uso de técnicas de encriptación y firma digital (ver también 10,3,2 y 10.3.3).

10.3.5 Administración de claves

10.3.5.1 Protección de claves criptográficas

La administración de claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. Cualquier compromiso o pérdida de claves criptográficas puede conducir a un compromiso de la confidencialidad, autenticidad y/o integridad de la información. Se debe implementar un sistema de administración para respaldar el uso por parte de la organización, de los dos tipos de técnicas criptográficas, los cuales son:

a) técnicas de clave secreta, cuando dos o más actores comparten la misma clave y esta se utiliza tanto para cifrar información como para descifrarla. Esta clave tiene que mantenerse en secreto dado que una persona que tenga acceso a la misma podrá descifrar toda la información cifrada con dicha clave, o introducir información no autorizada;
b) técnicas de clave publica, cuando cada usuario tiene un par de claves: una clave publica (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto). Las técnicas de clave publica pueden utilizarse para el cifrado (ver 10.3.2) y para generar firmas digitales (ver 10.3.3).

Todas las claves deben ser protegidas contra modificación y destrucción, y las claves secretas y privadas necesitan protección contra divulgación no autorizada.
Las técnicas criptográficas también pueden aplicarse con este propósito. Se debe proveer de protección física al equipamiento utilizado para generar, almacenar y archivar claves.

10.3.5.2 Normas, procedimientos y métodos

Un sistema de administración de claves debe estar basado en un conjunto acordado de normas, procedimientos y métodos seguros para:

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;
b) generar y obtener certificados de clave publica;
c) distribuir claves a los usuarios que corresponda, incluyendo como deben activarse las claves cuando se reciben;
d) almacenar claves, incluyendo como obtienen acceso a las claves los usuarios autorizados;
e) cambiar o actualizar claves incluyendo reglas sobre cuando y como deben cambiarse las claves;
f) ocuparse de las claves comprometidas;
g) revocar claves incluyendo como deben retirarse o desactivarse las mismas, por ej. cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deben archivarse);
h) recuperar claves perdidas o alteradas como parte de la administración de la continuidad del negocio, por ej. la recuperación de la información cifrada;
i) archivar claves, por ej. , para la información archivada o resguardada;
j) destruir claves;
k) registrar (logging) y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves deben tener fechas de entrada en vigencia y de fin de vigencia, definidas de manera que solo puedan ser utilizadas por un periodo limitado de tiempo. Este periodo debe definirse según el riesgo percibido y las circunstancias bajo las cuales se aplica el control criptográfico.

Podría resultar necesario considerar procedimientos para administrar requerimientos legales de acceso a claves criptográficas, por ej. puede resultar necesario poner a disposición la información cifrada en una forma clara, como evidencia en un caso judicial.

Además de la administración segura de las claves secretas y privadas, también debe tenerse en cuenta la protección de las claves publicas. Existe la amenaza de que una persona falsifique una firma digital reemplazando la clave publica de un usuario con su propia clave. Este problema es abordado mediante el uso de un certificado de clave publica. Estos certificados deben generarse en una forma que vincule de manera única la información relativa al propietario del par de claves publica/privada con la clave publica. En consecuencia es importante que el proceso de administración que genera estos certificados sea confiable. Normalmente, este proceso es llevado a cabo por una autoridad de certificación, la cual

debe residir en una organización reconocida, con adecuados controles y procedimientos implementados, para ofrecer el nivel de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicios o contratos con proveedores externos de servicios criptográficos, por ej. con una autoridad de certificación, deben comprender los tópicos de responsabilidad legal, confiabilidad del servicio y tiempos de respuesta para la prestación de los mismos (ver 4.2.2).

10.4 Seguridad de los archivos del sistema

Objetivo: Garantizar que los proyectos y actividades de soporte de TI se lleven a cabo de manera segura. Se debe controlar el acceso a los archivos del sistema. El mantenimiento de la integridad del sistema debe ser responsabilidad de la función usuaria o grupo de desarrollo a quien pertenece el software o sistema de aplicación.

10.4.1 Control del software operativo

Se debe proveer de control para la implementación de software en los sistemas en operaciones. A fin de minimizar el riesgo de alteración de los sistemas operacionales se deben tener en cuenta los siguientes controles:

a) La actualización de las bibliotecas de programas operativos solo debe ser realizada por el bibliotecario designado una vez autorizada adecuadamente por la gerencia (ver 10.4.3).
b) Si es posible, los sistemas en operaciones sólo deben guardar el código ejecutable.
c) El código ejecutable no debe ser implementado en un sistema operacional hasta tanto no se obtenga evidencia del éxito de las pruebas y de la aceptación del usuario, y se hayan actualizado las correspondientes bibliotecas de programas fuente.
d) Se debe mantener un registro de auditoria de todas las actualizaciones a las bibliotecas de programas operativos.
e) Las versiones previas de software deben ser retenidas como medida de contingencia.

El mantenimiento del software suministrado por el proveedor y utilizado en los sistemas operacionales debe contar con el soporte del mismo. Cualquier decisión referida a una actualización a una nueva versión debe tomar en cuenta la seguridad, por ej. la introducción de una nueva funcionalidad de seguridad o el número y la gravedad de los problemas de seguridad que afecten esa versión. Los parches de software deben aplicarse cuando pueden ayudar a eliminar o reducir las debilidades en materia de seguridad.

Solo debe otorgarse acceso lógico o físico a los proveedores con fines de soporte y si resulta necesario, y previa aprobación de la gerencia. Las actividades del proveedor deben ser monitoreadas.

10.4.2 Protección de los datos de prueba del sistema

Los datos de prueba deben ser protegidos y controlados. Las pruebas de aceptación del sistema normalmente requieren volúmenes considerables de datos de prueba, que sean tan cercanos como sea posible a los datos operativos. Se debe evitar el uso de bases de datos operativas que contengan información personal. Si se utiliza información de esta índole, esta debe ser despersonalizada antes del uso. Se deben aplicar los siguientes controles para proteger los datos operativos, cuando los mismos se utilizan con propósitos de prueba.

a) Los procedimientos de control de accesos, que se aplican a los sistemas de aplicación en operación, también deben aplicarse a los sistemas de aplicación de prueba.

b) Se debe llevar a cabo una autorización por separado cada vez que se copia información operativa a un sistema de aplicación de pruebas.
c) Se debe borrar la información operativa de un sistema de aplicación de prueba inmediatamente después de completada la misma.
d) La copia y el uso de información operacional deben ser registrado a fin de suministrar una pista de auditoria.

10.4.3 Control de acceso a las bibliotecas de programa fuente

A fin de reducir la probabilidad de alteración de programas de computadora, se debe mantener un control estricto del acceso a las bibliotecas de programa fuente, según los siguientes puntos (ver también el punto 8.3).

a) Dentro de lo posible, las bibliotecas de programas fuente no deben ser almacenadas en los sistemas que está operativo.
b) Se debe designar a un bibliotecario de programas para cada aplicación.
c) El personal de soporte de TI no debe tener acceso irrestricto a las bibliotecas de programas fuente.
d) Los programas en desarrollo o mantenimiento no deben ser almacenados en las bibliotecas de programas fuente operacional.
e) La actualización de bibliotecas de programas fuente y la distribución de programas fuente a los programadores, solo debe ser llevada a cabo por el bibliotecario designado, con la autorización del gerente de soporte de TI para la aplicación pertinente.
f) Los listados de programas deben ser almacenados en un ambiente seguro (ver 8.6.4).
g) Se debe mantener un registro de auditoria de todos los accesos a las bibliotecas de programa fuente.
h) Las viejas versiones de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en operaciones, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.
i) El mantenimiento y la copia de las bibliotecas de programas fuente deben estar sujeta a procedimientos estrictos de control de cambios (ver 10.4.1).

10.5 Seguridad de los procesos de desarrollo y soporte

Objetivo: Mantener la seguridad del software y la información del sistema de aplicación.
Se deben controlar estrictamente los entornos de los proyectos y el soporte a los mismos.
Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte. Los gerentes deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo.

10.5.1 Procedimientos de control de cambios

A fin de minimizar la alteración de los sistemas de información, debe existir un control estricto de la implementación de los cambios. Se debe imponer el cumplimiento de los procedimientos formales de control de cambios. Estos deben garantizar que no se comprometan los procedimientos de seguridad y control, que los programadores de soporte solo tengan acceso a aquellas partes del sistema necesarias para el desempeño de sus tareas, y que se obtenga un acuerdo y aprobación formal para cualquier cambio. Los cambios en el software de aplicaciones pueden tener repercusiones en el ambiente operativo. Siempre que resulte factible, los procedimientos de control de cambios operativos y de aplicaciones deben estar integrados (ver también 8.1.2). Este proceso debe incluir:

a) mantener un registro de los niveles de autorización acordados;

b) garantizar que los cambios son propuestos por usuarios autorizados;
c) revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios;
d) identificar todo el software, la información, las entidades de bases de datos y el hardware que requieran correcciones;
e) obtener aprobación formal para las propuestas detalladas antes de que comiencen las tareas;
f) garantizar que el usuario autorizado acepte los cambios antes de cualquier implementación;
g) garantizar que la implementación se lleve a cabo minimizando la discontinuidad de las actividades de la empresa;
h) garantizar que la documentación del sistema será actualizada cada vez que se completa un cambio y se archiva o elimina la documentación vieja;
i) mantener un control de versiones para todas las actualizaciones de software;
j) mantener una pista de auditoria de todas las solicitudes de cambios;
k) garantizar que la documentación operativa (ver 8.1.1) y los procedimientos de usuarios se modifiquen según las necesidades de adecuación;
l) garantizar que la implementación de cambios tenga lugar en el momento adecuado y no altere los procesos comerciales involucrados.

Muchas organizaciones mantienen un ambiente en el cual los usuarios prueban nuevo software y que esta separado de los ambientes de desarrollo y producción. Esto proporciona un medio para controlar el nuevo software y permitir la protección adicional de la información operacional que se utiliza con propósitos de prueba.

10.5.2 Revisión técnica de los cambios en el sistema operativo

Periódicamente es necesario cambiar el sistema operativo, por ej. instalar una versión nueva de software o parches. Cuando se realizan los cambio, los sistemas de aplicación deben ser revisados y probados para garantizar que no se produzca un impacto adverso en las operaciones o en la seguridad. Este proceso debe cubrir:

a) revisión de procedimientos de integridad y control de aplicaciones para garantizar que estos no hayan sido comprometidos por los cambios del sistema operativo;
b) garantizar que el plan y presupuesto de soporte anual contemple las revisiones y las pruebas del sistema que deban realizarse como consecuencia del cambio en el sistema operativo;
c) garantizar que se notifiquen los cambios del sistema operativo de manera oportuna antes de la implementación;
d) garantizar que se realicen cambios apropiados en los planes de continuidad de la empresa (ver punto 11).

10.5.3 Restricción del cambio en los paquetes de software

Se debe desalentar la realización de modificaciones a los paquetes de software. En la medida de lo posible, y de lo viable, los paquetes de software suministrados por proveedores deben ser utilizados sin modificación. Cuando se considere esencial modificar un paquete de software, se deben tener en cuenta los siguientes puntos:

a) el riesgo de compromiso de los procesos de integridad y controles incorporados;
b) si se debe obtener el consentimiento del proveedor;
c) la posibilidad de obtener del proveedor los cambios requeridos como actualizaciones estándar de programas;
d) el impacto que se produciría si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios se consideran esenciales, se debe retener el software original y aplicar los cambios a una copia claramente identificada. Todos los cambios deben ser probados y documentados exhaustivamente, de manera que pueden aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software.

10.5.4 Canales ocultos y código troyano

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos.

Puede activarse modificando un parámetro accesible mediante elementos tanto seguros como no seguros de un sistema informático, o incorporando información a un flujo de datos. El código troyano esta diseñado para afectar un sistema en una forma no autorizada, no fácilmente advertida y no requerida por el destinatario o usuario del programa. Los canales ocultos y el código troyano raramente surgen por accidente. Si se aborda este tópico, se deben considerar los siguientes puntos:

a) solo comprar programas de proveedores acreditados;
b) comprar programas en código fuente de manera que el mismo pueda ser verificado;
c) utilizar productos evaluados;
d) examinar todo el código fuente antes de utilizar operativamente el programa;
e) controlar el acceso y las modificaciones al código una vez instalado el mismo;
f) emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

10.5.5 Desarrollo externo de software

Cuando se terceriza el desarrollo de software, se deben considerar los siguientes puntos:

a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual (ver 12.1.2);
b) certificación de la calidad y precisión del trabajo llevado a cabo;
c) acuerdos de custodia en caso de quiebra de la tercera parte;
d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;
e) requerimientos contractuales con respecto a la calidad del código;
f) realización de pruebas previas a la instalación para detectar códigos troyanos.

11 ADMINISTRACIÓN DE LA CONTINUIDAD DE LOS NEGOCIOS

11.1 Aspectos de la administración de la continuidad de los negocios

Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.
Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ej., desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptables mediante una combinación de controles preventivos y de recuperación.
Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio. Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.
La administración de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

11.1.1 Proceso de administración de la continuidad de los negocios

Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad de los negocios en toda la organización. Este debe contemplar los siguientes aspectos clave de la administración de la continuidad:

a) Comprensión de los riesgos que enfrenta la organización en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios;
b) comprensión del impacto que una interrupción puede tener en los negocios (es importante que se encuentren soluciones para los incidentes menos significativos, así como para los incidentes graves que podrían amenazar la viabilidad de la organización) y definición de los objetivos comerciales de las herramientas de procesamiento de información;
c) considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio;
d) elaboración y documentación de una estrategia de continuidad de los negocios consecuente con los objetivos y prioridades de los negocios acordados;
e) elaboración y documentación de planes de continuidad del negocio de conformidad con la estrategia de continuidad acordada;
f) pruebas y actualización periódicas de los planes y procesos implementados;
g) garantizar que la administración de la continuidad de los negocios esté incorporada a los procesos y estructura de la organización. La responsabilidad por la coordinación del proceso de administración de la continuidad debe ser asignada a un nivel jerárquico adecuado dentro de la organización, por ej. al foro de seguridad de la información (ver 4.1.1).

11.1.2 Continuidad del negocio y análisis del impacto

La continuidad de los negocios debe comenzar por la identificación de eventos que puedan ocasionar interrupciones en los procesos de los negocios, por ej. fallas en el equipamiento, inundación e incendio. Luego debe llevarse a cabo una evaluación de riesgos para determinar el impacto de dichas interrupciones (tanto en términos de magnitud de daño como del período de recuperación). Estas dos actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. Esta evaluación considera todos los procesos de negocio y no se limita a las instalaciones de procesamiento de la información.
Según los resultados de la evaluación, debe desarrollarse un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de los negocios. Una vez que se ha creado este plan, el mismo debe ser aprobado por la gerencia.

11.1.3 Elaboración e implementación de planes de continuidad de los negocios

Los planes deben ser desarrollados para mantener o restablecer las operaciones de los negocios en los plazos requeridos una vez ocurrida una interrupción o falla en los procesos críticos de los negocios. El proceso de planificación de la continuidad de los negocios debe considerar los siguientes puntos:

a) identificación y acuerdo con respecto a todas la responsabilidades y procedimientos de emergencia;
b) implementación de procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de la dependencias de negocios externos y a los contratos vigentes;
c) documentación de los procedimientos y procesos acordados;

d) instrucción adecuada del personal en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis;
e) prueba y actualización de los planes.

El proceso de planificación debe concentrarse en los objetivos de negocio requeridos, por ej. restablecimiento de los servicios a clientes en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia ("fallback") en sitios alternativos de procesamiento de la información.

11.1.4 Marco para la planificación de la continuidad de los negocios

Se debe mantener un solo marco para los planes de continuidad de los negocios, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento. Cada plan de continuidad debe especificar claramente las condiciones para su puesta en marcha, así como las personas responsables de ejecutar cada componente del mismo. Cuando se identifican nuevos requerimientos, deben modificarse de conformidad los procedimientos de emergencia establecidos, por ej. los planes de evacuación o los recursos de emergencia ("fallback") existentes.
El marco para la planificación de la continuidad de los negocios debe tener en cuenta los siguientes puntos:

a) las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos;
b) procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la empresa y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ej. policía, bomberos y autoridades locales;
c) procedimientos de emergencia ("fallback") que describan las acciones a emprender para el traslado de actividades esenciales de la empresa o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos de negocio en los plazos requeridos;
d) procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la empresa;
e) un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo:
f) actividades de concientización e instrucción que estén diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces;
g) las responsabilidades de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan. Se deben mencionar alternativas cuando corresponda.

Cada plan debe tener un propietario específico. Los procedimientos de emergencia, los planes de reanudación ("fallback") y los planes de recuperación deben contarse entre las responsabilidades de los propietarios de los recursos o procesos de negocio pertinentes. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios

Los planes de continuidad de los negocios pueden fallar en el curso de las pruebas, frecuentemente debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal. Por

consiguiente deben ser probados periódicamente para garantizar que están actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.
El cronograma de pruebas para los planes de continuidad del negocio debe indicar cómo y cuándo debe probarse cada elemento del plan. Se recomienda probar con frecuencia cada uno de los componentes del plan. Se deben utilizar diversas técnicas para garantizar que los planes funcionarán en la vida real. Estas deben incluir:}

a) pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplo de interrupciones);
b) simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis);
c) pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia);
d) pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal);
e) pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído);
f) ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones);

Estas técnicas pueden ser utilizadas por cualquier organización y deben reflejar la naturaleza del plan de recuperación pertinente.

11.1.5.1 Mantenimiento y reevaluación del plan

Los planes de continuidad de los negocios deben mantenerse mediante revisiones y actualizaciones periódicas para garantizar su eficacia permanente. Se deben incluir procedimientos en el programa de administración de cambios de la organización para garantizar que se aborden adecuadamente los tópicos de continuidad del negocio.

Se debe asignar la responsabilidad por las revisiones periódicas de cada uno de los planes de continuidad del negocio; la identificación de cambios en las disposiciones relativas al negocio aún no reflejadas en los planes de continuidad debe seguirse de una adecuada actualización del plan. Este proceso formal de control de cambios debe garantizar que se distribuyan los planes actualizados y que se imponga el cumplimiento de los mismos mediante revisiones periódicas de todos los planes.

Entre los ejemplos de situaciones que podrían demandar la actualización de los planes se encuentra la adquisición de nuevo equipamiento, o la actualización (“upgrading”) de los sistemas operacionales y los cambios de:

a) personal
b) direcciones o números telefónicos;
c) estrategia de los negocios;
d) ubicación, instalaciones y recursos;
e) legislación;
f) contratistas, proveedores y clientes clave;
g) procesos, o procesos nuevos/eliminados;
h) riesgos (operacionales y financieros).

12 CUMPLIMIENTO

12.1 Cumplimiento de requisitos legales

Objetivo: Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.
El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.
Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados. Los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ej. flujo de datos a través de fronteras).

12.1.1 Identificación de la legislación aplicable

Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información. Del mismo modo deben definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.

12.1.2 Derechos de propiedad intelectual (DPI)

12.1.2.1 Derecho de propiedad intelectual

Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derecho de propiedad intelectual, derechos de diseño o marcas registradas. La infracción de derechos de autor (derecho de propiedad intelectual) puede tener como resultado acciones legales que podrían derivar en demandas penales.

Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por la organización, o material autorizado o suministra-do a la misma por la empresa que lo ha desarrollado.

12.1.2.2 Derecho de propiedad intelectual del software

Los productos de software que constituyan propiedad de una empresa se suministran normalmente bajo un acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede limitar la copia a la creación de copias de resguardo solamente. Se deben considerar los siguientes controles:

a) publicación de una política de cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software;
b) emisión de estándares para los procedimientos de adquisición de productos de software;
c) mantenimiento de la concientización respecto de las políticas de adquisición y derecho de propiedad intelectual de software, y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el cumplimiento de las mismas;
d) mantenimiento adecuados de registros de activos;
e) mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
f) implementación de controles para garantizar que no se exceda el número máximo permitido de usuarios;

g) comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;
h) emisión de una política para el mantenimiento de condiciones adecuadas con respecto a las licencias;
i) emisión de una política con respecto a la eliminación o transferencia de software a terceros;
j) utilización de herramientas de auditoría adecuadas;
k) cumplimiento de términos y condiciones con respecto a la obtención de software e información en redes públicas (ver también el punto 8.7.6).

12.1.3 Protección de los registros de la organización

Los registros importantes de la organización deben protegerse contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del negocio. Un ejemplo de esto son los registros que pueden requerirse como evidencia de que una organización opera dentro de un determinado marco legal o normativo, o para garantizar una adecuada defensa contra eventuales acciones civiles o penales, o para validar el estado financiero de una organización ante accionistas, socios y auditores. El plazo y el contenido de los datos para la retención de información pueden ser establecidos por leyes o normas nacionales.

Los registros deben ser clasificados en diferentes tipos, por ej. registros contables, registros de base de datos, “logs” de transacciones, “logs” de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ej. papel, microfichas, medios magnéticos u ópticos. Las claves criptográficas asociadas con archivos cifrados o firmas digitales (ver 10.3.2 y 10.3.3) deben mantenerse en forma segura y estar disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación deben implementarse de acuerdo con las recomendaciones del fabricante.

Si se seleccionan medios de almacenamiento electrónicos, deben incluirse procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas pro futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos deben seleccionarse de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ej. que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación debe garantizar una clara identificación de los registros y de su período de retención legal o normativa. Debe permitir una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para la organización.

A fin de cumplir con estas obligaciones, se deben tomar las siguientes medidas dentro de la organización.

a) Se debe emitir lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información;
b) Se debe preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Se debe mantener un inventario de fuentes de información clave.

d) Se debe implementar adecuados controles para proteger los registros y la información esenciales contra pérdida, destrucción y falsificación.

12.1.4 Protección de datos y privacidad de la información personal

Diversos países han introducido leyes que establecen controles sobre el procesamiento y transmisión de datos personales (generalmente información sobre personas vivas que pueden ser identificadas a partir de esta información). Dichos controles pueden imponer responsabilidades a aquellas personas que recopilan, procesan y divulgan información personal, y pueden limitar la capacidad de transferir dichos datos a otros países.

El cumplimiento de la legislación sobre protección de datos requiere una estructura y un control de gestión adecuados. Frecuentemente, esto se logra de la mejor manera mediante la designación de un responsable a cargo de la protección de datos que oriente a los gerentes, usuarios y prestadores de servicios acerca de sus responsabilidades individuales y de los procedimientos específicos que deben seguirse. Debe ser responsabilidad del propietario de los datos, informar al responsable de la protección de los mismos, acerca de las propuestas para mantener la información personal, en un archivo estructurado, y para garantizar el conocimiento de los principios de protección de datos, definidos en la legislación pertinente.

12.1.5 Prevención del uso inadecuado de los recursos de procesamiento de información

Los recursos de procesamiento de información de una organización se suministran con propósitos de negocio. La gerencia debe autorizar el uso que se da a los mismos. La utilización de estos recursos con propósitos no autorizados o ajenos a los negocios, sin la aprobación de la gerencia, debe ser considerada como uso indebido. Si dicha actividad es identificada mediante monitoreo u otros medios, se debe notificar al gerente interesado para que se tomen las acciones disciplinarias que correspondan.

La legalidad del monitoreo del uso de los recursos mencionados varía según el país y puede requerir que los empleados sean advertidos de dichas actividades o que se obtenga el consentimiento de los mismos. Se debe obtener asesoramiento jurídico antes de implementar los procedimientos de monitoreo.
Muchos países tienen, o están en proceso de introducir, legislación referida a la protección contra el uso inadecuado de los recursos informáticos. El uso de los mismos con propósitos no autorizados puede constituir un delito criminal. Por consiguiente, es esencial que todos los usuarios estén al corriente del alcance preciso del acceso permitido. Esto puede lograrse, por ejemplo, otorgando a los usuarios una autorización escrita, una copia de la cual debe ser firmada por los mismos y retenida en forma segura por la organización. Los empleados y los usuarios externos deber ser advertidos de la prohibición de todo acceso que no esté expresamente autorizado.

En el momento del inicio de sesión debe aparecer un mensaje de advertencia en pantalla indicando que el sistema al que se está ingresando es privado y que no se permite el acceso no autorizado. El usuario debe acusar recepción y responder en forma adecuada al mensaje para continuar con el proceso de inicio de sesión.

12.1.6 Regulación de controles para el uso de criptografía

Algunos países han implementado acuerdos, leyes, normas y demás instrumentos para controlar el acceso a los controles criptográficos o el uso de los mismos. Dicho control puede incluir:

a) importación y/o exportación de hardware y software para desempeñar funciones criptográficas;

b) importación y/o exportación de hardware y software diseñado para aceptar funciones criptográficas;
c) métodos obligatorios o discrecionales de acceso de los países a la información cifrada por hardware y software para proveer de confidencialidad al contenido.

Se debe procurar asesoramiento jurídico para garantizar el cumplimiento de las leyes nacionales. También debe obtenerse asesoramiento antes de transferir a otro país la información cifrada o los controles criptográficos.

12.1.7 Recolección de evidencia

12.1.7.1 Reglas para la recolección de evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implica la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con las normas de evidencia establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso. En general, estas normas comprenden:

a) validez de la evidencia: si puede o no utilizarse la misma en el tribunal;
b) peso de la evidencia: la calidad y totalidad de la misma;
c) adecuada evidencia de que los controles han funcionado en forma correcta y consistente (por ej. evidencia de control de procesos) durante todo el período en que la evidencia a recuperar fue almacenada y procesada por el sistema.

12.1.7.2 Validez de la evidencia

Para lograr la validez de la evidencia, las organizaciones deben garantizar que sus sistemas de información cumplan con los estándares o códigos de práctica relativos a la producción de evidencia válida.

12.1.7.3 Calidad y totalidad de la evidencia

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. En general, esta pista puede establecerse si se cumplen las siguientes condiciones:

a) Para documentos en papel: el original se almacena en forma segura y se mantienen registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.
b) Para información en medios informáticos: se deben hacer copias de los medios removibles y de la información en discos rígidos o en memoria para garantizar su disponibilidad. Se debe mantener un registro de todas las acciones realizadas durante el proceso de copia y éste debe ser presenciado. Se debe almacenar en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente puede no resultar obvio si éste derivará en una demanda legal. Por consiguiente, existe el riesgo de que la evidencia necesaria sea destruida accidentalmente antes de que se advierta la gravedad del incidente. Es aconsejable involucrar a un abogado o a la policía en la primera etapa de cualquier acción legal contemplada y procurar asesoramiento acerca de la evidencia requerida.

12.2 Revisiones de la política de seguridad y la compatibilidad técnica

Objetivo: Garantizar la compatibilidad de los sistemas con las políticas y estándares (normas) de seguridad de la organización.
La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes y las plataformas técnicas y sistemas de información deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad.

12.2.1 Cumplimiento de la política de seguridad

La gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Asimismo, se debe considerar la implementación de una revisión periódica de todas las áreas de la organización para garantizar el cumplimiento de las políticas y estándares de seguridad. Entre las áreas a revisar deben incluirse las siguientes:

a) sistemas de información;
b) proveedores de sistemas;
c) propietarios de información y de recursos de información;
d) usuarios;
e) gerentes.

Los propietarios de los sistemas de información (ver 5.1) deben apoyar la revisión periódica de la conformidad de sus sistemas con las políticas, estándares y otros requisitos de seguridad aplicables. El tópico referido al monitoreo operacional del uso del sistema es tratado en el punto 9.7.

12.2.2 Verificación de la compatibilidad técnica

Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad. La verificación de la compatibilidad técnica comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de cumplimiento requiere asistencia técnica especializada. Debe ser realizada manualmente (si es necesario, con el apoyo de adecuadas herramientas de software) por un ingeniero en sistemas experimentado, o por un paquete de software automatizado que genere un informe técnico para su ulterior interpretación por parte de un especialista.

La verificación de compatibilidad también puede comprender pruebas de penetración, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito.

Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas. Se deben tomar recaudos en caso de que una prueba de penetración exitosa pueda comprometer la seguridad del sistema e inadvertidamente permita explotar otras vulnerabilidades,

Las verificaciones de compatibilidad técnica sólo deben ser realizadas por personas competentes y autorizadas o bajo la supervisión de las mismas.

12.3 Consideraciones de auditoria de sistemas

Objetivo: Optimizar la eficacia del proceso de auditoria de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditorias de sistemas.
Asimismo, se requiere una protección adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoria.

12.3.1 Controles de auditoria de sistemas

Los requerimientos y actividades de auditoria que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio. Se deben contemplar los siguientes puntos:

a) Los requerimientos de auditoria deben ser acordados con la gerencia que corresponda;
b) se debe acordar y controlar el alcance de las verificaciones;
c) éstas deben estar limitadas a un acceso de sólo lectura del software de datos;
d) el acceso que no sea de sólo lectura solamente debe permitirse para copias aisladas de archivos del sistema, las cuales deben ser eliminadas una vez finalizada la auditoría.
e) se deben identificar claramente y poner a disposición los recursos de TI para llevar a cabo las verificaciones;
f) se deben identificar y acordar los requerimientos de procesamiento especial o adicional;
g) todos los accesos deben ser monitoreados y registrados a fin de generar una pista de referencia;
h) se deben documentar todos los procedimientos, requerimientos y responsabilidades.

12.3.2 Protección de las herramientas de auditoría de sistemas

Se debe proteger el acceso a las herramientas de auditoría de sistemas, por ej. archivos de datos o software, a fin de evitar el mal uso o el compromiso de las mismas. Dichas herramientas deben estar separadas de los sistemas operacionales y de desarrollo y no deben almacenarse en bibliotecas de cintas o en áreas de usuarios, a menos que se les otorgue un nivel adecuado de protección adicional.

Anexo A
(Informativo)

Bibliografía

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
ISO/IEC 17799:2000 - Information technology. Code of practice for information security management.

Anexo B
(Informativo)

El estudio de este esquema ha estado a cargo del Subcomité de Seguridad de la información, integrado de la forma siguiente:

Integrante	**Representa a:**
Lic. Adalberto AIRALA	UNIV. TECN. NAC. - FAC. REG. BS. AS.
Dr. Daniel ALTMARK	COLEGIO DE ABOGADOS
Lic. Juan de Dios BEL	ISACA - INFORMATION SYSTEMS AUDIT. AND CONTROL ASSOCIATION
Sr. Osvaldo PÉREZ	IEEE ARGENTINA
Sr. Rodrigo SEGUEL	SECRET. DE MODERNIZACIÓN DEL ESTADO
Dr. Pablo TISCORNIA	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Lic. Juan Carlos MASOERO	IRAM
Lic. Jorge NUNES	IRAM
Lic. Espedito PASSARELLO	IRAM

TRÁMITE

El estudio de esta norma fue considerado por el Subcomité en sus reuniones del 2002-02-28 (Acta 1-2002) y 2002-03-21 (Acta 2-2002) en la que se aprobó como Esquema 1 para su envío a Discusión Pública por 45 d.

****

APROBADO SU ENVIO A DISCUSIÓN PÚBLICA POR EL SUBCOMITÉ DE SEGURIDAD DE LA INFORMACIÓN, EN SU SESIÓN DEL 21 DE MARZO DE 2002 (Acta 2-2002).

FIRMADO
Lic. Jorge Nunes
Lic. Juan C. Masoero
Coordinador del Subcomité

FIRMADO
Lic. Juan Bel
Secretario del Subcomité

FIRMADO
Lic. Marta R. de Barbieri
Vº Bº Equipo A