

Contenido

		Página
	Preámbulo	IV
0	Introducción	1
1	Alcance y campo de aplicación	6
2	Términos y definiciones	6
3	Política de seguridad	7
4	Seguridad organizacional	8
4.1	Infraestructura de la seguridad de la información	8
4.2	Seguridad del acceso de una tercera parte	12
4.3	Externalización	15
5	Clasificación y control de bienes	17
5.1	Responsabilidad de los bienes	17
5.2	Clasificación de la información	18
6	Seguridad del personal	19
6.1	Seguridad en la definición del trabajo y recursos	19
6.2	Entrenamiento del usuario	21
6.3	Respuesta a los incidentes de seguridad y malfuncionamiento	22
7	Seguridad física y del ambiente	24
7.1	Areas seguras	24

	Página
7.2	Seguridad de los equipos 27
7.3	Controles generales 32
8	Gestión de las operaciones y de las comunicaciones 33
8.1	Responsabilidades y procedimientos de las operaciones 33
8.2	Aceptación y planificación del sistema 38
8.3	Protección contra el software malicioso 40
8.4	Administración interna 41
8.5	Gestión de red 43
8.6	Seguridad y manipulación de dispositivos 43
8.7	Intercambios de información y software 46
9	Control de acceso 53
9.1	Requisitos del negocio para el control de acceso 53
9.2	Gestión de acceso de usuario 54
9.3	Responsabilidades del usuario 57
9.4	Control de acceso a la red 59
9.5	Control de acceso a la operación del sistema 64
9.6	Control de acceso a la aplicación 68
9.7	Monitoreo de uso y acceso al sistema 69
9.8	Computadores móviles y teletrabajo 73
10	Desarrollo y mantenimiento de sistemas 75
10.1	Requisitos de seguridad de los sistemas 75

Contenido

	Página
10.2	Seguridad de las aplicaciones de los sistemas 76
10.3	Controles criptográficos 79
10.4	Seguridad de los archivos de sistema 83
10.5	Seguridad en los procesos de desarrollo y apoyo 86
11	Gestión de la continuidad del negocio 89
12	Cumplimiento 93
12.1	Cumplimiento con los requisitos legales 93
12.2	Revisión de las políticas de seguridad y cumplimiento técnico 98
12.3	Consideraciones sobre la auditoría del sistema 100

Tecnología de la información - Código de práctica para la gestión de seguridad de la información

Preámbulo

El Instituto Nacional de Normalización, INN, es el organismo que tiene a su cargo el estudio y preparación de las normas técnicas a nivel nacional. Es miembro de la INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) y de la COMISION PANAMERICANA DE NORMAS TECNICAS (COPANT), representando a Chile ante esos organismos.

La norma NCh2777 - ISO/IEC 17799: 2000 ha sido preparada por la División de Normas del Instituto Nacional de Normalización, y en su estudio participaron los organismos y las personas naturales siguientes:

Armada de Chile
Banco del Estado
Banco Santander
Cámara Nacional de Comercio - ONCE

Certibanc - Enable
Corporación de Fomento de la Producción, CORFO
Corporación de Investigación Tecnológica de Chile - INTEC

e-Cert Chile
Instituto Nacional de Normalización, INN

Ministerio de Salud - DIPLAP
Orión
Orión 2000
Servicio de Impuestos Internos, SII

Bernard Johnson H.
Héctor Monje V.
Marcelo Muñoz A.
Bernardino Arance M.
Paula Silva B.
Roberto Riveros D.
Paul Saffery G.
Verónica Acha A.
Patricio Escobar R.
Esteban Segura R.
Leonor Ceruti M.
Jorge Muñoz C.
Andrés Tabja R.
Christian Yáñez V.
Claudio Ordóñez U.
Andrés Boré P.
Fernando Barraza L.
Jaime Labbé S.

Subsecretaría de Economía
 Subsecretaría de Telecomunicaciones
 Subsecretaría Secretaría General de la Presidencia

Superintendencia de Bancos e Instituciones Financieras
 Universidad de Santiago - Depto. de Ingeniería Informática
 Universidad Técnica Federico Santa María - Depto. de Industrias

Raúl Arrieta C.
 Claudio Pezoa L.
 Daniel Cortés E.
 Gonzalo Martner F.
 Renato Córdova G.
 Rogers Atero
 Alejandro Bedini

Esta norma se estudió para establecer las recomendaciones sobre la gestión de seguridad de la información para las personas responsables de implementar y mantener esta seguridad en la organización.

Esta norma es una homologación de la Norma Internacional ISO/IEC 17799: 2000 Information technology - Code of practice for information security management, siendo idéntica a la misma.

Sin embargo, al estudiar la norma ISO/IEC 17799: 2000 para adoptarla como norma chilena, el Comité Técnico del INN que analizó esta norma acordó:

- no traducir ciertos términos debido a que son de uso común en la literatura técnica;
- traducir algunos términos indicando el término original en inglés para un mejor entendimiento;
- incluir los términos indicados en los puntos anteriores en una tabla en el preámbulo de la norma para no modificar la norma ISO/IEC 17799:2000, ya que esta norma chilena es una homologación idéntica a la misma.

Término en inglés (ISO/IEC 17799: 2000)	Término utilizado en la norma chilena	Otros términos de uso habitual en el país
management	dirección/gestión	gerencia/ administración
manager	directivo, encargado	gerente
fora, forum	comité	foro
denial of service attack	ataque de denegación de servicio	ataque de negación de servicio
hacking	hacking	piratería
user IDs	user IDs	identificación de usuario
worms	worms	gusanos
courier	courier	mensajero, correo
token	token	dispositivo de hardware
smart card	tarjeta inteligente	
batch	batch	por lotes
logged on	sesión abierta	
logged out	sesión cerrada	
logged back	sesión reiniciada	
firewall	firewall	equipo muro cortafuego
gateway	gateway	equipo puerta de acceso
time slot	intervalo de tiempo	
joint venture	joint venture	socio del negocio
call forwarding	desvío de llamadas	

NCh2777

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 27 de Diciembre de 2002.

Esta norma ha sido declarada Oficial de la República de Chile por Resolución Exenta N°92, de fecha 07 de Marzo de 2003, del Ministerio de Economía, Fomento y Reconstrucción, publicada en el Diario Oficial del 13 de Marzo de 2003.

Tecnología de la información - Código de práctica para la gestión de seguridad de la información

0 Introducción

¿Qué es la seguridad de la información?

La información es un bien que, como otros bienes del negocio, tiene valor para una organización y consecuentemente necesita ser protegida en forma apropiada. La seguridad de la información protege la información de una amplia gama de amenazas con el fin de asegurar la continuidad del negocio, minimizar el daño del negocio y maximizar el retorno de la inversión y las oportunidades del negocio.

La información puede existir de muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquier forma que tome la información, o los dispositivos por los cuales es compartida o almacenada, siempre debería estar protegida en forma adecuada.

La seguridad de la información se caracteriza aquí como la preservación de la:

- a) confidencialidad: asegurar que la información sea accesible sólo por aquellos usuarios autorizados para tener acceso;
- b) integridad: salvaguardar que la información y los métodos de procesamiento sean exactos y completos;
- c) disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

La seguridad de la información se logra mediante la implementación de un adecuado conjunto de controles, los que podrían ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Se necesita establecer estos controles para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

¿Por qué es necesaria la seguridad de la información?

La información y los procesos de apoyo, sistemas y redes son importantes bienes del negocio. La confidencialidad, integridad y disponibilidad de la información puede ser esencial para mantener el margen de competitividad, flujo de caja, utilidad, cumplimiento legal e imagen del negocio.

Las organizaciones y sus sistemas de información y redes están enfrentados en forma creciente a las amenazas de la seguridad desde una amplia gama de fuentes, incluyendo fraudes apoyados por computador, espionaje, sabotaje, vandalismo, fuego o inundación. Las fuentes de daño tales como los virus computacionales, hacking por computador y ataques de denegación de servicio han llegado a ser más comunes, más ambiciosas y cada vez más sofisticadas.

La dependencia en los sistemas de información y de servicios implica que las organizaciones son más vulnerables a amenazas de seguridad. La interconexión de las redes públicas y privadas y la compartición de los recursos de la información, aumenta la dificultad de lograr el control de acceso. La tendencia a los sistemas de computación distribuidos ha debilitado la efectividad del control central especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que se puede lograr a través de dispositivos técnicos es limitada, y debería ser apoyada por procedimientos y una gestión apropiada. Identificar qué controles y en qué lugar deberían estar, requiere una planificación cuidadosa y una atención detallada. La gestión de seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. Puede también requerir la participación de los proveedores, clientes o accionistas. También pueden ser necesarias las opiniones de especialistas de organizaciones externas.

Los controles de seguridad de la información son considerablemente más baratos y más efectivos si son incorporados en la etapa de diseño y especificación de los requisitos.

¿Cómo establecer los requisitos de seguridad?

Es esencial que una organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

La primera fuente se obtiene al evaluar los riesgos para la organización. A través de esta evaluación, se identifican las amenazas a los bienes, la vulnerabilidad, se evalúa la probabilidad de ocurrencia y se estima el impacto potencial.

La segunda fuente es la legal, estatutaria, regulatoria y los requisitos contractuales que tiene que satisfacer tanto la organización, como sus socios comerciales, los proveedores y personal externo de servicios.

La tercera fuente es un conjunto particular de principios, objetivos y requisitos para el procesamiento de la información que una organización ha desarrollado para el apoyo de sus operaciones.

Evaluación de los riesgos de la seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos de ella. El gasto en los controles es necesario compararlo con el probable perjuicio que resulte de fallas en la seguridad. Las técnicas de evaluación de los riesgos se pueden aplicar a toda la organización, o solamente a partes de ella, como también a los sistemas de información individuales, componentes específicos de un sistema o servicios, cuando sea práctico, realista y útil.

La evaluación del riesgo es la consideración sistemática de:

- a) El probable perjuicio al negocio que resulte de una falla en la seguridad, tomando en cuenta las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad de la información y otros bienes.
- b) La probabilidad realista de que tal falla ocurra, en vista de las amenazas y vulnerabilidades efectivas, y los controles actualmente implementados.

Los resultados de esta evaluación serán una guía y determinarán la acción de una gestión apropiada, así como las prioridades de la gestión de los riesgos de seguridad de la información, y la selección de la implementación de controles para protegerla de estos riesgos. Puede ser necesario realizar varias veces el proceso de evaluación de los riesgos y seleccionar los controles para cubrir diferentes partes de la organización o sistemas de información individuales.

Es importante realizar revisiones periódicas de los riesgos de la seguridad e implementar controles para:

- a) tomar en cuenta los cambios de las prioridades y requisitos del negocio;
- b) considerar nuevas amenazas y vulnerabilidades;
- c) confirmar que los controles permanecen efectivos y apropiados.

Las revisiones se deberían realizar en diferentes niveles de profundidad, dependiendo de los resultados de las evaluaciones previas y de los cambios de niveles de riesgo que la dirección está preparada para aceptar. Las evaluaciones del riesgo, a menudo se realizan primero a alto nivel, como una forma de priorizar los recursos en áreas de alto riesgo, y luego en un nivel más detallado, para abordar riesgos específicos.

Selección de controles

Una vez que los requisitos de seguridad se hayan identificado, se deberían seleccionar e implementar los controles para asegurar que los riesgos se reduzcan a un nivel aceptable. Los controles se pueden seleccionar de este documento o de otro conjunto de controles, cuando sea apropiado, o de controles nuevos que se puedan diseñar para cumplir las necesidades específicas. Hay diferentes formas de gestionar los riesgos y este documento provee ejemplos de enfoques habituales. Sin embargo, es necesario reconocer que algunos de los controles no son aplicables a todos los sistemas o ambientes de información, y pueden no ser prácticos para todas las organizaciones. Como un ejemplo, en 8.14 se describe cómo las obligaciones pueden ser separadas para prevenir fraudes y errores. Para pequeñas organizaciones puede ser imposible separar todas las obligaciones y pueden ser necesarias otras formas de alcanzar el mismo objetivo de control. Como otro ejemplo en 9.7 y 12.1, se describe cómo el uso del sistema puede ser monitoreado y así reunir las evidencias necesarias. Los controles descritos, por ejemplo, el registro de eventos, pueden estar en conflicto con la legislación aplicable, tal como la protección a la privacidad de los clientes o la de los lugares de trabajo.

Los controles se deberían seleccionar en base a los costos de implementación en relación al riesgo que se va a reducir y las pérdidas potenciales si ocurre una violación de la seguridad. También se deberían tomar en cuenta los factores no monetarios tales como la pérdida de reputación.

Algunos de los controles en este documento se pueden considerar como principios guías para la gestión de seguridad de la información y aplicables a la mayoría de las organizaciones. Ellos están explicados en más detalle a continuación con el título Punto de partida de la seguridad de la información.

Punto de partida de la seguridad de la información

Se puede considerar como principio guía cierto número de controles que proveen un buen punto de partida para la implementación de la seguridad de la información. Ellos están basados en los requisitos legislativos esenciales o que se consideran comúnmente como la mejor práctica de seguridad de la información.

Los controles considerados como esenciales en una organización, desde el punto de vista legislativo, incluyen:

- a) protección de los datos y privacidad de la información personal (ver 12.1.4);
- b) salvaguardia de los registros de la organización (ver 12.1.3);
- c) derechos de propiedad intelectual (ver 12.1.2).

Los controles considerados comúnmente como la mejor práctica de seguridad de la información, incluyen:

- a) documentación de la política de seguridad de la información (ver 3.1);
- b) asignación de responsabilidades en la seguridad de la información (ver 4.1.3);

- c) educación y entrenamiento en la seguridad de la información (ver 6.2.1);
- d) informes de incidentes en la seguridad (ver 6.3.1);
- e) gestión de continuidad del negocio (ver 11.1).

Estos controles se aplican en la mayoría de las organizaciones y en la mayoría de los ambientes. Se debería tener presente que aunque todos los controles en este documento son importantes, la relevancia de algún control se debería determinar en vista del riesgo específico que una organización está enfrentando. De aquí que, aunque el tratamiento anterior se considera un buen punto de partida, esto no reemplaza la selección de controles en base a una evaluación del riesgo.

Factores críticos para el éxito

La experiencia ha mostrado que los siguientes factores a menudo son críticos en la implementación exitosa de la seguridad de la información dentro de una organización:

- a) política, objetivos y actividades de seguridad que reflejen los objetivos del negocio;
- b) una aproximación para la implementación de la seguridad que sea consistente con la cultura organizacional;
- c) apoyo visible y compromiso de la dirección;
- d) buen entendimiento de los requisitos de seguridad, evaluación y gestión del riesgo;
- e) difusión efectiva de la seguridad por todos los directivos y empleados;
- f) distribución de las normas y de la guía de la política de seguridad de la información a todos los empleados y personal externo;
- g) provisión de entrenamiento y educación adecuada;
- h) utilización de un sistema de medición equilibrado y completo para evaluar el comportamiento de la gestión de seguridad de la información y la realimentación de sugerencias para su mejoramiento.

Desarrollo de guías propias

Este código de práctica se puede considerar como un punto de partida para desarrollar una guía en una organización específica. No toda la guía y los controles de este código pueden ser aplicables. Por lo tanto, pueden ser necesarios controles adicionales no incluidos en este documento. Cuando esto suceda, puede ser útil conservar referencias cruzadas que faciliten la verificación del cumplimiento por parte de los auditores y socios del negocio.

1 Alcance y campo de aplicación

Esta norma establece las recomendaciones para la gestión de seguridad de información por quienes son responsables de iniciar, implementar y mantener la seguridad en la organización.

Esta norma entrega una base común para desarrollar las normas de seguridad de la organización y una práctica efectiva de gestión de seguridad y establecer confianza en las relaciones entre las organizaciones.

Las recomendaciones de esta norma se deben seleccionar y usar de acuerdo con las leyes y reglamentos aplicables.

2 Términos y definiciones

Para los propósitos de esta norma, se aplican los términos y definiciones siguientes:

2.1 confidencialidad: aseguramiento de que la información sea accesible sólo por quienes están autorizados para tener acceso

2.2 disponibilidad: aseguramiento de que los usuarios tengan acceso a la información y bienes asociados cuando lo necesiten

2.3 evaluación del riesgo: cuantificación de las amenazas de impactar y vulnerar la información y las instalaciones de procesamiento de la información y la probabilidad de ocurrencia

2.4 gestión del riesgo: proceso de identificación, control y minimización o eliminación de los riesgos de la seguridad que pueden afectar los sistemas de información, a un costo aceptable

2.5 integridad: salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento

2.6 seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información

3 Política de seguridad

3.1 Política de seguridad de la información

Objetivo: Fijar la orientación y el apoyo de la dirección a la seguridad de la información.

La dirección debería fijar una política de orientación clara y demostrar el apoyo y el compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información en toda la organización.

3.1.1 Documentación de la política de seguridad de la información

La dirección debería aprobar un documento de la política de seguridad, publicarlo y comunicarlo, cuando sea apropiado, a todos los empleados. Esto establecería un compromiso de la dirección y fijaría el tratamiento de la organización para gestionar la seguridad de la información. Como mínimo, se debería incluir la guía siguiente:

- a) una definición de seguridad de la información, sus objetivos globales y alcance y la importancia de la seguridad como un mecanismo que permita compartir la información (ver introducción);
- b) una declaración de intención de la dirección, como apoyo a las metas y principios de la seguridad de la información;
- c) una breve explicación de las políticas de seguridad, principios, normas y requisitos de cumplimiento necesarios de particular importancia en la organización, por ejemplo:
 - c.1) cumplimiento con los requisitos legislativos y contractuales;
 - c.2) requisitos de educación en la seguridad;
 - c.3) prevención y detección de virus y otros software maliciosos;
 - c.4) gestión de la continuidad del negocio;
 - c.5) consecuencias de las violaciones a la política de seguridad;
- d) una definición de las responsabilidades generales y específicas de gestión de seguridad de la información, que incluya un informe de incidentes en la seguridad;
- e) referencias a la documentación que puede apoyar la política, por ejemplo, políticas de seguridad más detalladas y procedimientos para sistemas de información específicos o reglas de seguridad que debieran cumplir los usuarios.

Esta política se debería comunicar a los usuarios de toda la organización en una forma que sea pertinente, accesible y entendible por el lector objetivo.

3.1.2 Revisión y evaluación

La política debería tener un dueño el cual es responsable de su mantenimiento y revisión de acuerdo al proceso de revisión definido. Este proceso debería asegurar que se realiza una revisión en respuesta a cualquier cambio que afecte las bases de la evaluación original del riesgo, por ejemplo, incidentes significativos en la seguridad, nuevas vulnerabilidades o cambios en la infraestructura técnica u organizacional. Se debería además tener un cronograma de revisiones periódicas sobre lo siguiente:

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

4 Seguridad organizacional

4.1 Infraestructura de la seguridad de la información

Objetivo: Gestionar la seguridad de la información dentro de la organización.

Se debería establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Se debería constituir un comité adecuado con líderes de la dirección para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implementación de la seguridad en toda la organización. Si es necesario, se deberían obtener consejos de especialistas en seguridad de la información que estén disponibles dentro de la organización.

Se deberían desarrollar contactos con especialistas externos en seguridad para estar al tanto de las tendencias industriales, normas de monitoreo y métodos de evaluación y proveer puntos de enlace apropiados cuando se traten los incidentes de la seguridad. Se debería estimular una aproximación multi disciplinaria a la seguridad de la información, por ejemplo, involucrar la cooperación y colaboración de los directivos, usuarios, administradores, diseñadores de aplicación, auditores, personal de seguridad y especialistas con experiencia en áreas tales como gestión de seguros y riesgos.

4.1.1 Comité de gestión de seguridad de la información

La seguridad de la información es una responsabilidad del negocio, compartida por todos los miembros del equipo de la dirección. Por lo tanto se debería considerar un comité de la dirección para asegurar que haya una orientación clara y un apoyo de la dirección, visible para las iniciativas de seguridad.

Este comité debería promover la seguridad dentro de la organización a través de compromisos apropiados y recursos adecuados. El comité puede ser parte de un grupo existente de la dirección. Típicamente, tal comité lleva a cabo lo siguiente:

- a) revisión y aprobación de la política de seguridad de la información y de las responsabilidades generales;
- b) monitoreo de los cambios significativos en la exposición de los bienes de información a amenazas mayores;
- c) revisión y monitoreo de los incidentes de seguridad de la información;
- d) aprobación de iniciativas importantes para mejorar la seguridad de la información.

Un directivo debería ser responsable de todas las actividades relacionadas con la seguridad.

4.1.2 Coordinación de la seguridad de la información

En una organización grande puede ser necesario un comité de representantes de la dirección con funciones transversales, de partes importantes de la organización, para coordinar la implementación de los controles de la seguridad de la información. Típicamente, tal comité:

- a) acuerda roles y responsabilidades específicos para la seguridad de la información en toda la organización;
- b) acuerda metodologías y procesos específicos para la seguridad de la información, por ejemplo, evaluación del riesgo, sistema de clasificación de la seguridad;
- c) acuerda y apoya las iniciativas de seguridad de la información en toda la organización, por ejemplo, un programa de sensibilización sobre seguridad;
- d) garantiza que la seguridad sea parte del proceso de planificación de la información;
- e) evalúa la adecuación de los controles de seguridad de una información específica, y coordina la implementación para los nuevos sistemas o servicios;
- f) revisa los incidentes de seguridad de la información;
- g) promueve la visibilidad del apoyo del negocio a la seguridad de la información en toda la organización.

4.1.3 Asignación de responsabilidades en la seguridad de la información

Deberían estar claramente definidas las responsabilidades para la protección de bienes individuales y para llevar a cabo procesos de seguridad específicos.

La política de seguridad de la información (ver cláusula 3) debería entregar una guía general en la asignación de responsabilidades en la organización. Esto se debería complementar, cuando sea necesario, con una guía más detallada de sitios, sistemas o servicios específicos. Deberían estar claramente definidas las responsabilidades locales para los bienes físicos individuales y de información, así como los procesos de seguridad, tales como la planificación de la continuidad del negocio.

En muchas organizaciones se designará un encargado de seguridad de la información, quien tomará toda la responsabilidad para el desarrollo e implementación de la seguridad y para apoyar en la identificación de los controles.

Sin embargo, la responsabilidad por los recursos y la implementación de los controles a menudo permanece en los directivos individuales. Una práctica habitual es designar un dueño para cada bien de información quien se hace responsable de su seguridad en el día a día.

Los dueños de los bienes de información pueden delegar sus responsabilidades de seguridad a los directivos individuales o proveedores de servicio. Sin embargo, el dueño permanece como último responsable de la seguridad del bien y debería ser capaz de determinar que la responsabilidad delegada se ha encargado correctamente.

Es esencial que las áreas de las cuales cada directivo es responsable estén claramente establecidas; en particular debería ocurrir lo siguiente:

- a) Se deberían identificar y definir claramente los diversos bienes y los procesos de seguridad asociados con cada sistema individual.
- b) El directivo responsable de cada bien o proceso de seguridad debería estar de acuerdo y debería documentar los detalles de esta responsabilidad.
- c) Los niveles de autorización se deberían definir claramente y documentar.

4.1.4 Procesos de autorización para las instalaciones de procesamiento de información

Se debería establecer una gestión del proceso de autorización para las instalaciones de procesamiento de información nuevas.

Se deberían considerar los controles siguientes:

- a) Las instalaciones nuevas deberían tener una apropiada aprobación de la dirección usuaria, autorización de su propósito y uso. Se debería obtener además la aprobación del directivo responsable del mantenimiento del ambiente de seguridad del sistema de información local, para asegurar que se cumplan todos los requisitos y políticas importantes de seguridad.
- b) Cuando sea necesario, se debería revisar el hardware y software para asegurar que sean compatibles con otros componentes del sistema.

NOTA - Para ciertas conexiones puede ser requerida una aprobación tipo.

- c) El uso de instalaciones de procesamiento de la información personal para el procesamiento de la información del negocio y cualquier control necesario debería ser autorizado.
- d) El uso de instalaciones de procesamiento de la información personal en los lugares de trabajo puede causar nuevas vulnerabilidades y por lo tanto deberían ser evaluadas y autorizadas.

Estos controles son especialmente importantes en un ambiente de red.

4.1.5 Consejo de un especialista en seguridad de la información

Probablemente en muchas organizaciones sea necesario el consejo de un especialista en seguridad. Idealmente, éste lo debería dar un asesor interno experimentado en seguridad. No todas las organizaciones pueden emplear a un asesor especialista, en tales casos, se recomienda que una persona específica con experiencia y conocimientos coordine internamente, para asegurar la consistencia, y proveer ayuda en la toma de decisiones relacionadas con la seguridad. Ellos deberían también tener acceso apropiado a las opiniones de los especialistas asesores externos, además de su experiencia.

Los asesores de seguridad de la información o las personas equivalentes de contacto deberían tener la misión de proveer consejos en todos los aspectos de la seguridad de la información, usando su propia opinión o la externa. La calidad de su evaluación de las amenazas a la seguridad y consejo sobre los controles determinará la efectividad de la seguridad de la información de la organización. Para una máxima efectividad e impacto, a ellos se les debería permitir el acceso directo a la gestión de toda la organización.

El asesor de seguridad de la información o la persona de contacto deberían ser consultados en la etapa más temprana posible a continuación de una sospecha de incidente o violación de la seguridad, para proveer una guía experta o recursos de investigación. Aunque la mayoría de las investigaciones internas de seguridad se realizarán normalmente bajo el control de la dirección, se puede llamar al consultor de seguridad de información para opinar, guiar o conducir la investigación.

4.1.6 Cooperación entre organizaciones

Se deberían mantener los contactos apropiados con las autoridades encargadas de la aplicación de las leyes, cuerpos regulatorios, proveedores de servicios de información y operadores de telecomunicaciones, para asegurar que en el evento de un incidente de seguridad se tomen rápidamente las acciones apropiadas, y se obtenga un consejo. Similarmente, se deberían considerar los miembros de los grupos de seguridad y de los comités de la industria.

Los intercambios de información de seguridad se deberían restringir para asegurar que la información confidencial de la organización no sea entregada a personas no autorizadas.

4.1.7 Revisión independiente de la seguridad de la información

Los documentos de la política (ver 3.1) de seguridad de la información, fijan la política y las responsabilidades de la seguridad de información. Su implementación se debería revisar independientemente para dar la garantía de que las prácticas de la organización reflejan apropiadamente la política, y que ésta es factible y efectiva (ver 12.2).

Tal revisión la puede realizar un auditor interno, un directivo independiente o una organización de tercera parte, especializada en tales revisiones, cuando estos candidatos tengan la habilidad y experiencia apropiada.

4.2 Seguridad del acceso de una tercera parte

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de información organizacional y de los bienes de información accedidos por terceras partes.

Se debería controlar el acceso de terceras partes a las instalaciones de procesamiento de información de la organización.

Cuando exista una necesidad del negocio para el acceso de una tercera parte, se debería realizar una evaluación del riesgo para determinar las implicancias en la seguridad y los requisitos de control. Los controles se deberían acordar y definir en un contrato con la tercera parte.

El acceso de la tercera parte también puede involucrar a otros participantes. Los contratos que otorgan accesos de terceras partes deberían incluir el permiso para designar a otros participantes elegibles y las condiciones para su acceso.

Esta norma se podría usar como base para tales contratos y cuando se considere la externalización del procesamiento de la información.

4.2.1 Identificación de los riesgos del acceso de una tercera parte

4.2.1.1 Tipos de acceso

El tipo de acceso dado a una tercera parte es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos que resultan de un acceso físico. Los tipos de acceso que se deberían considerar son:

- a) acceso físico, por ejemplo, a las oficinas, salas de computadores, gabinetes de archivos;
- b) acceso lógico, por ejemplo a una base de datos, a los sistemas de información de una organización.

4.2.1.2 Razones para el acceso

A las terceras partes se les puede conceder acceso por varias razones. Por ejemplo, existe una tercera parte que provee servicios para una organización y no está ubicada en el sitio, a ellos se les puede dar acceso lógico y físico, tales como:

- a) personal de apoyo de software y hardware, quien necesita acceso a nivel de sistema o a bajo nivel de funcionalidad de la aplicación;
- b) a los socios del negocio o joint ventures, quienes pueden intercambiar información, acceder a los sistemas de información o compartir bases de datos.

La información se puede poner en riesgo debido al acceso de terceras partes, por una inadecuada gestión de seguridad. Cuando hay una necesidad del negocio para conectar un sitio de una tercera parte, se debería realizar una evaluación del riesgo para identificar cualquier requisito de control específico. Se debería tomar en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y las implicancias de este acceso a la seguridad de la información de la organización.

4.2.1.3 Personal externo en el sitio

Las terceras partes que están ubicadas en el sitio por un período de tiempo definido en sus contratos, también pueden dar origen a una debilidad de la seguridad. Los ejemplos de terceras partes en el sitio incluyen:

- a) personal de apoyo y mantenimiento de hardware y software;
- b) servicios de aseo, de alimentación, guardias de seguridad y otros servicios de apoyo externalizados;
- c) empleo de estudiantes y otros empleos ocasionales de corto tiempo;
- d) consultores.

Es esencial entender que los controles son necesarios para administrar el acceso de la tercera parte a las instalaciones de procesamiento de información. Generalmente, todos los requisitos de seguridad o controles internos que resultan del acceso de la tercera parte se deberían reflejar en el contrato de esta tercera parte (ver 4.2.2). Por ejemplo, si hay una necesidad especial de confidencialidad de la información, se puede usar un acuerdo de no divulgación (ver 6.1.3).

El acceso por terceras partes a la información y a las instalaciones de procesamiento de información, no se debería autorizar hasta que se hayan implementado los controles apropiados y se haya firmado un contrato definiendo los términos de la conexión o acceso.

4.2.2 Requisitos de seguridad en los contratos con terceras partes

Los convenios que involucran el acceso de una tercera parte a las instalaciones de procesamiento de la información organizacional, deberían estar basados en un contrato formal que contenga o haga referencia a todos los requisitos de seguridad para asegurar el cumplimiento de las políticas y normas de seguridad de la organización. El contrato debería asegurar que no haya malos entendidos entre la organización y la tercera parte. Las organizaciones deberían satisfacer por sí mismas cómo serán indemnizadas por sus proveedores. Se deberían considerar los términos siguientes para incluirlos en el contrato:

- a) política general de la seguridad de la información;
- b) protección de los bienes, incluyendo:
 - b.1) procedimientos para proteger los bienes de la organización, incluyendo la información y el software;
 - b.2) procedimientos para determinar si ha ocurrido algún compromiso en los bienes, por ejemplo, pérdida o modificación de los datos;
 - b.3) controles para asegurar la devolución o destrucción de la información y bienes al final del contrato, o de común acuerdo, en una fecha durante la vigencia del mismo;
 - b.4) integridad y disponibilidad;
 - b.5) restricciones en el copiado y divulgación de la información;
- c) una descripción de cada servicio que va a estar disponible;
- d) el nivel presupuestado del servicio y los niveles inaceptables;
- e) estipulación de transferencia de personal cuando sea apropiado;
- f) las respectivas obligaciones de las partes en el acuerdo;
- g) responsabilidades con respecto a las materias legales, por ejemplo, legislación de protección de los datos, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el contrato involucra la cooperación con organizaciones de otros países (ver 12.1);
- h) derechos de propiedad intelectual (DPIs) y asignación de los derechos de autor (ver 12.1.2) y protección de cualquier trabajo colaborativo (ver también 6.1.3);

- i) acuerdos de control de acceso, que cubran:
 - i.1) los métodos de acceso permitidos y el control y uso de identificadores únicos tales como user IDs y contraseñas;
 - i.2) un proceso de autorización para el acceso y privilegios de usuario;
 - i.3) un requisito de mantener una lista de las personas autorizadas a usar los servicios que se hagan disponibles y cuáles son sus derechos y privilegios con respecto a tal uso;
- j) la definición de un criterio verificable de comportamiento, su monitoreo e informe;
- k) el derecho para monitorear y revocar la actividad del usuario;
- l) el derecho para auditar las responsabilidades contractuales o realizar estas auditorías mediante una tercera parte;
- m) el establecimiento de un proceso de escalamiento para la resolución de problemas; también se deberían considerar, cuando sea apropiado disposiciones de contingencia;
- n) responsabilidades concernientes a la instalación y mantenimiento de hardware y software;
- o) una clara estructura de informes y formatos acordados por las partes;
- p) un proceso de gestión de cambio claro y específico;
- q) cualquier control necesario de protección física y los mecanismos para asegurar que estos controles se cumplan;
- r) entrenamiento en los métodos, procedimientos y seguridad al usuario y administrador;
- s) controles para asegurar la protección contra software maliciosos (ver 8.3);
- t) disposiciones para informar, notificar e investigar los incidentes y las violaciones a la seguridad;
- u) involucramiento de la tercera parte con el personal externo.

4.3 Externalización

Objetivo: Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información se haya externalizado a otra organización.

Las disposiciones de externalización deberían consignar en el contrato entre las partes los riesgos, los controles de seguridad y los procedimientos para los sistemas de información, ambientes de redes y/o computadores personales.

4.3.1 Requisitos de seguridad en los contratos de externalización

Los requisitos de seguridad de una organización que externaliza la gestión y control de todos o algunos de sus sistemas de información, ambientes de redes y/o computadores personales se deberían consignar en un contrato acordado entre las partes.

Por ejemplo, el contrato debería consignar:

- a) cómo se van a cumplir los requisitos legales, por ejemplo, la legislación de protección de datos;
- b) qué disposiciones tendrán lugar para asegurar que todas las partes involucradas en la externalización, incluidos los subcontratistas, están conscientes de sus responsabilidades en la seguridad;
- c) cómo se van a mantener y probar la integridad y la confidencialidad de los bienes del negocio de la organización;
- d) qué controles físicos y lógicos se usarán con los usuarios autorizados, para restringir y limitar el acceso a la información sensible del negocio de la organización;
- e) cómo se va a mantener la disponibilidad de los servicios en el evento de un desastre;
- f) qué niveles de seguridad física se suministrarán para los equipos externalizados;
- g) el derecho de auditar.

Los términos indicados en la lista en 4.2.2 también se deberían considerar como parte de este contrato. El contrato debería permitir que los requisitos de seguridad y los procedimientos puedan ser desarrollados en un plan de gestión de seguridad a ser acordado entre las dos partes.

Aunque los contratos de externalización pueden plantear algunas preguntas complejas de seguridad, los controles incluidos en este código de práctica podrían servir como un punto de partida para acordar la estructura y contenido del plan de gestión de seguridad.

5 Clasificación y control de bienes

5.1 Responsabilidad de los bienes

Objetivo: Mantener una protección apropiada de los bienes de la organización.

Todos los bienes de información importantes se deberían contabilizar y deberían tener designado un dueño.

La responsabilidad de los bienes ayuda a asegurar que se mantenga la protección apropiada. Se deberían identificar los dueños de todos los bienes importantes y se debería asignar la responsabilidad del mantenimiento de los controles apropiados. Se puede delegar la responsabilidad de la implementación de los controles. La responsabilidad debería permanecer con el dueño designado del bien.

5.1.1 Inventario de los bienes

El inventario de los bienes ayuda a asegurar que se realice una protección efectiva de los bienes y también puede ser necesario para otros propósitos del negocio, tales como salud y seguridad, razones financieras o de seguros (gestión del bien). El proceso de recopilar un inventario de bienes es un aspecto importante de gestión del riesgo. Una organización necesita ser capaz de identificar sus bienes y el valor relativo e importancia de ellos. Basada en esta información una organización puede así proveer niveles de protección en proporción con el valor e importancia de los bienes. Se debería implementar y mantener un inventario de los bienes importantes asociados con cada sistema de información. Cada bien se debería identificar claramente, documentar y acordar su propiedad y su clasificación de seguridad (ver 5.2), junto con su actual ubicación (importante cuando se intenta recuperar de una pérdida o daño). Ejemplos de bienes asociados con los sistemas de información son:

- a) bienes de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, material de entrenamiento, procedimientos de apoyo y operación, planes de continuidad, planes de recuperación, información archivada;
- b) bienes de software: software de aplicación, software de sistema, herramientas de desarrollo y utilitarios;
- c) bienes físicos: equipos de computación (procesadores, monitores, computadores portátiles, modems), equipos de comunicación (ruteadores, PABXs, máquinas de fax, máquinas contestadoras), medios magnéticos (cintas y discos), otros equipos técnicos (fuentes de alimentación, unidades de aire acondicionado), mobiliario;
- d) servicios: servicios de computación y comunicaciones, servicios públicos en general, por ejemplo, calefacción, iluminación, energía eléctrica, aire acondicionado.

5.2 Clasificación de la información

Objetivo: Asegurar que los bienes de información reciban un nivel apropiado de protección.

La información se debería clasificar para indicar la necesidad, prioridad y grado de protección.

La información tiene un grado de sensibilidad y criticidad variable. Algunos ítemes pueden requerir un nivel adicional de protección o una manipulación especial. Se debería usar un sistema de clasificación para definir un conjunto apropiado de niveles de protección, y comunicar la necesidad de medidas especiales de manipulación.

5.2.1 Guías para la clasificación

La clasificación y los controles de protección asociados a la información, deberían tomar en cuenta la necesidad del negocio de compartir o restringir la información, y los impactos del negocio asociados con tales necesidades, por ejemplo, acceso no autorizado o daño a la información. En general, la clasificación dada a la información es una forma resumida de determinar cómo se debe manipular y proteger esta información.

La información y las salidas de los sistemas que manipulan los datos clasificados se deberían etiquetar en términos de su valor y sensibilidad para la organización. Puede ser también apropiado etiquetar la información en términos de cuán crítica es para la organización, por ejemplo, en términos de su integridad y disponibilidad.

La información a menudo deja de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos se deberían tomar en cuenta, ya que una sobre-clasificación puede llevar a un gasto adicional innecesario del negocio. Las guías de clasificación deberían anticipar y permitir el hecho que la clasificación de cualquier ítem dado de la información no es necesariamente fija durante todo el tiempo, y puede cambiar de acuerdo con alguna política predeterminada (ver 9.1).

Se debería dar cierta consideración al número de categorías de clasificación y a los beneficios que se ganan con su uso. Esquemas demasiado complejos pueden llegar a ser engorrosos y no económicos para su uso o ser poco prácticos. Se debería tener cuidado en interpretar las etiquetas de clasificación en los documentos de otras organizaciones que pueden tener diferentes definiciones para la misma etiqueta o algunas denominadas similarmente.

La responsabilidad para definir la clasificación de un ítem de información, por ejemplo, para un documento, registro de dato, archivo de datos o diskette, y para la revisión periódica de esa clasificación, debería permanecer con el creador o dueño nominado de la información.

5.2.2 Etiquetado y manipulación de la información

Es importante que se defina un conjunto apropiado de procedimientos para el etiquetado y la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización. Estos procedimientos necesitan cubrir los bienes de información en formatos físicos y electrónicos. Para cada clasificación, se debería definir los procedimientos de manipulación para cubrir los siguientes tipos de actividad de procesamiento de la información:

- a) copiado;
- b) almacenamiento;
- c) transmisión por correo tradicional, fax y correo electrónico;
- d) transmisión de voz, incluyendo teléfono móvil, correo de voz y máquinas contestadoras;
- e) destrucción.

La salida de los sistemas que contienen información que está clasificada como sensible o crítica debería tener una etiqueta apropiada de clasificación (en la salida). La etiqueta debería reflejar la clasificación de acuerdo a las reglas establecidas en 5.2.1. Los ítemes a considerar incluyen los informes impresos, pantallas de computador, medios magnéticos (cintas, discos, CDs, cassettes), mensajes electrónicos y transferencias de archivos.

Las etiquetas físicas son generalmente las formas más apropiadas de etiquetar. Sin embargo, algunos bienes de información, tales como documentos en forma electrónica, no se pueden etiquetar físicamente y se deben usar dispositivos de etiquetado electrónico.

6 Seguridad del personal

6.1 Seguridad en la definición del trabajo y recursos

Objetivo: Reducir los riesgos de error humano, robos, fraudes o mal uso de las instalaciones.

Las responsabilidades de seguridad se deberían asignar en la etapa de contratación del personal, incluirlas en los contratos, y monitorearlas durante el empleo de la persona.

Los potenciales postulantes se deberían seleccionar adecuadamente (ver 6.1.2), especialmente para trabajos sensibles. Todos los empleados y los usuarios de terceras partes de los equipos de procesamiento de la información, deberían firmar un acuerdo de confidencialidad (no divulgación).

6.1.1 Incorporación de la seguridad en las responsabilidades del trabajo

Los roles de seguridad y responsabilidad, como se establecen en la política de seguridad de la información de la organización (ver 3.1), se deberían documentar cuando sea apropiado. Ellos deberían incluir cualquier responsabilidad general para implementar o mantener la política de seguridad como también cualquier responsabilidad específica para la protección de los bienes particulares, o por la ejecución de actividades o procesos de seguridad particulares.

6.1.2 Selección y política de personal

Se deberían realizar verificaciones al personal permanente al momento de la contratación. Esto debería incluir los controles siguientes:

- a) disponibilidad de referencias satisfactorias, por ejemplo, una comercial y una personal;
- b) una verificación (de la totalidad y exactitud) del currículum vitae del postulante;
- c) confirmación de las calificaciones profesionales y académicas exigidas;
- d) verificación de identidad (pasaporte, cédula de identidad o documento similar).

Cuando un trabajo, ya sea en una designación inicial o en una promoción, involucra a una persona que tiene acceso a los equipos de procesamiento de la información, y en particular si hay una manipulación de información sensible, por ejemplo, información financiera o altamente confidencial, la organización debería realizar una revisión de los antecedentes financieros. Para el personal que es autoridad importante, esta revisión se debería repetir periódicamente.

Se debería realizar un proceso de selección similar para el personal temporal y externo. Cuando este personal es empleado a través de una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de ella en los procedimientos de selección y notificación, que necesitan seguir si la selección no ha sido completa o si los resultados son dudosos.

La dirección debería evaluar la supervisión necesaria para el personal nuevo y sin experiencia con autorización para acceder a sistemas sensibles. El trabajo de todo el personal debería estar sujeto a revisiones periódicas y aprobación de los procedimientos por un miembro más antiguo.

Los directivos deberían estar conscientes que circunstancias personales de su personal pueden afectar su trabajo. Problemas financieros, personales, cambios en su comportamiento o estilo de vida, ausencias recurrentes y evidencias de estrés o depresión podrían llevar a un fraude, robo, error u otras implicancias en la seguridad. Esta información se debería tratar de acuerdo con alguna legislación aplicable, en la jurisdicción pertinente.

6.1.3 Acuerdos de confidencialidad

Los acuerdos de confidencialidad o de no divulgación, se usan para notificar que la información es secreta o confidencial. Los empleados deberían normalmente firmar un acuerdo como parte de los términos y condiciones iniciales de empleo.

El personal temporal y los usuarios de terceras partes no cubiertos por un contrato existente (que contenga un acuerdo de confidencialidad), deberían firmar un acuerdo de confidencialidad antes de que tengan acceso a los equipos de procesamiento de la información.

Los acuerdos de confidencialidad se deberían revisar cuando haya cambios de las condiciones del empleo o contrato, particularmente cuando los empleados deben dejar la organización por alguna razón o por término de contrato.

6.1.4 Términos y condiciones de contratación

Los términos y condiciones de contratación deberían establecer la responsabilidad en la seguridad de la información. Cuando sea apropiado, estas responsabilidades continuarían por un tiempo definido después de finalizar la contratación. Se debería incluir la acción que se tomará si el empleado descuida los requisitos de seguridad.

También se deberían aclarar e incluir en los términos y condiciones de contratación, las responsabilidades y derechos legales del empleado, por ejemplo, leyes relacionadas con los derechos de propiedad o la legislación de protección de datos. También se debería incluir la responsabilidad por la clasificación y gestión de los datos del empleador. Se debería establecer, cuando sea apropiado, que los términos y condiciones de contratación se extiendan fuera de las instalaciones de la organización y fuera de las horas normales de trabajo, por ejemplo, en caso de trabajos en la casa (ver también 7.2.5 y 9.8.1).

6.2 Entrenamiento del usuario

Objetivo: Asegurar que los usuarios estén conscientes de las amenazas de la seguridad de la información y lo que afecta y estén equipados para apoyar la política de seguridad de la organización durante su trabajo normal.

Los usuarios se deberían entrenar en los procedimientos de seguridad y en el uso correcto de los equipos de procesamiento de la información para minimizar los posibles riesgos en la seguridad.

6.2.1 Educación y entrenamiento en la seguridad de la información

Todos los empleados de la organización y los usuarios de terceras partes, deberían recibir cuando sea pertinente, un entrenamiento adecuado y actualizaciones regulares de los procedimientos y políticas de la organización. Esto incluye los requisitos de seguridad, las responsabilidades legales y controles del negocio, así como el entrenamiento en el uso correcto de los equipos de procesamiento de la información, por ejemplo, el procedimiento de ingreso, uso de paquetes de software, después que se haya otorgado el acceso a la información o a los servicios.

6.3 Respuesta a los incidentes de seguridad y malfuncionamiento

Objetivo: Minimizar el daño de los incidentes de seguridad y malfuncionamientos, monitorear y aprender de tales incidentes.

Los incidentes que afectan la seguridad se deberían informar tan rápido como sea posible, a través de un canal de gestión apropiado.

Todos los empleados y personal externo deberían estar conscientes de los procedimientos de informe de los diferentes tipos de incidentes (violación de la seguridad, amenaza, debilidad o malfuncionamientos) que podrían tener un impacto en la seguridad de los bienes de la organización. Se les debería exigir que informen a la persona designada de contacto cualquier incidente que se observe o sea sospechoso tan rápido como sea posible. La organización debería establecer un proceso disciplinario formal para las relaciones con los empleados quienes cometan violaciones a la seguridad. Para ser capaz de guiar los incidentes en forma apropiada después de la ocurrencia, puede ser necesario reunir evidencias tan pronto como sea posible (ver 12.1.7).

6.3.1 Informes de incidentes de seguridad

Los incidentes de seguridad se deberían informar a través de canales de gestión apropiados tan rápido como sea posible.

Se debería establecer un procedimiento formal de informes, junto con un procedimiento de respuesta al incidente y disponer la acción a tomar cuando se reciba un informe. Todos los empleados y personal externo deberían estar conscientes del procedimiento de informes de incidentes de seguridad, y se les debería exigir que informen tales incidentes tan rápido como sea posible. Se deberían implementar procesos de realimentación convenientes para asegurar que estos informes de incidentes sean contrastados con los resultados después que el incidente se haya tratado y cerrado. Estos incidentes se pueden usar en entrenamientos de sensibilización del usuario (ver 6.2) como ejemplos de lo que podría suceder, cómo responder a tales incidentes, y cómo evitar la ocurrencia en el futuro (ver 12.1.7).

6.3.2 Informes de deficiencias de la seguridad

Se les debería exigir a los usuarios de los servicios de información que registren e informen cualquier deficiencia observada o sospechosa de la seguridad, o amenazas a los servicios o sistemas. Ellos deberían informar estas materias a su dirección o directamente a su proveedor de servicio tan rápido como sea posible. A los usuarios se les debería informar que en ninguna circunstancia ellos deberían, intentar probar una deficiencia sospechosa. Por su propia protección, una prueba de la deficiencia se podría interpretar como un potencial mal uso del sistema.

6.3.3 Informe de malfuncionamientos del software

Se deberían establecer los procedimientos para informar los malfuncionamientos del software. Se deberían considerar las acciones siguientes:

- a) Se deberían registrar los síntomas del problema y cualquier mensaje que aparezca en la pantalla.
- b) Se debería aislar el computador, si es posible, y detener su uso. Se debería informar al contacto apropiado de inmediato. Si el equipo se va a examinar, se debería desconectar de cualquier red de la organización antes de volver a energizarlo. Los diskettes no se deberían transferir a otro computador.
- c) Se debería informar inmediatamente el tema al encargado de seguridad de la información.

Los usuarios no deberían intentar retirar el software sospechoso, a menos que estén autorizados para realizarlo. El personal apropiadamente entrenado y experimentado debería realizar la recuperación del software.

6.3.4 Aprendizaje de los incidentes

Debería existir en el lugar de trabajo los mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y malfuncionamientos. Esta información se debería usar para identificar malfuncionamientos o incidentes recurrentes o de alto impacto. Esto puede indicar la necesidad de reforzar los controles o agregar controles adicionales para limitar la frecuencia, daño y costo de ocurrencias futuras, o para ser tomados en cuenta en los procesos de revisión de la política de seguridad (ver 3.1.2).

6.3.5 Procesos disciplinarios

Debería existir un proceso disciplinario formal para los empleados que hayan violado las políticas y procedimientos de seguridad (ver 6.1.4 y para la conservación de la evidencia ver 12.1.7). Tal proceso puede actuar como un disuasivo para los empleados quienes de otra forma podrían estar inclinados a descuidar los procedimientos de seguridad. Adicionalmente, esto debería asegurar un trato adecuado a los empleados quienes son sospechosos de cometer violaciones serias o persistentes a la seguridad.

7 Seguridad física y del ambiente

7.1 Áreas seguras

Objetivo: Prevenir el acceso no autorizado, daño e interferencia a las instalaciones del negocio y a la información.

Los equipos de procesamiento de información crítica o sensible del negocio, se deberían mantener en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de seguridad y controles de entrada. Estos deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

La protección provista debería ser en proporción con los riesgos identificados. Una política de escritorio y pantalla limpia se recomienda para reducir el riesgo de acceso no autorizado o daño a papeles, dispositivos y equipos de procesamiento de información.

7.1.1 Perímetro de seguridad físico

La protección física se puede lograr por la creación de varias barreras físicas alrededor de las instalaciones del negocio y de los equipos de procesamiento de información. Cada barrera establece un perímetro de seguridad aumentando la protección total provista. Las organizaciones deberían usar los perímetros de seguridad para proteger áreas que contengan los equipos de procesamiento (ver 7.1.3). Un perímetro de seguridad es algo que establece una barrera, por ejemplo, una pared, una puerta de entrada controlada por tarjeta o una recepción atendida. La ubicación y la resistencia de cada barrera dependen de los resultados de la evaluación del riesgo.

Se deberían considerar e implementar cuando sean apropiadas, las guías y controles siguientes:

- a) Debería estar claramente definido el perímetro de seguridad.
- b) El perímetro de un edificio o sitio que contiene equipos de procesamiento de información debería estar físicamente íntegro (es decir, no debería haber brechas en el perímetro o áreas donde fácilmente podría ocurrir una intromisión). Las paredes externas del sitio deberían ser de construcción sólida y todas las puertas externas deberían estar protegidas en forma adecuada del acceso no autorizado, por ejemplo, con mecanismos de control, barras, alarmas, cerrojos, etc.
- c) Debería existir en el sitio, un área de recepción atendida u otros medios para controlar el acceso físico al sitio o edificio. El acceso a los edificios y sitios se debería restringir de tal forma que solamente ingrese el personal autorizado.

- d) Si es necesario, las barreras físicas se deberían extender desde los pisos reales a los cielos reales para evitar la entrada de personas no autorizadas y la contaminación del ambiente tal como la causada por el fuego o inundación.
- e) Todas las puertas contra fuego en el perímetro de seguridad deberían tener alarma y cerrar de un golpe.

7.1.2 Controles físicos de entrada

Las áreas seguras se deberían proteger con controles de entrada apropiados para asegurar que solamente personal autorizado tenga permitido el acceso. Se deberían considerar los controles siguientes:

- a) Para asegurar las áreas, las visitas se deberían supervisar o autorizar, registrar su fecha y hora de entrada y salida. El acceso de las visitas se debería permitir solamente para propósitos autorizados y específicos y se debería otorgar con instrucciones de los requisitos de seguridad y procedimientos de emergencia del área.
- b) Los accesos a la información sensible, y a los equipos de procesamiento de información, se deberían controlar y restringir de tal forma que solamente ingresen personas autorizadas. Se deberían usar los controles de autenticación, por ejemplo, una tarjeta magnética más el PIN, para autorizar y validar todos los accesos. Se debería mantener en forma segura un registro de todos los accesos.
- c) Se debería exigir a todo el personal llevar la identificación en forma visible y se debería estimular para que exijan a los extraños no acompañados y a cualquiera que no lleve la identificación visible a que lo haga.
- d) Se deberían revisar y modificar regularmente los derechos de acceso a las áreas seguras.

7.1.3 Oficinas, salas e instalaciones seguras

Un área segura puede ser una oficina cerrada con llave o varias salas en el interior del perímetro de seguridad física, que pueden ser cerradas con llaves y puede contener gabinetes con llave o cajas fuerte. La selección y diseño de un área segura debería tomar en cuenta la posibilidad de daño por fuego, inundación, explosión, desorden civil y otras formas de desastres naturales o hechos por el hombre. También se debería tomar en cuenta las normas y reglas pertinentes a la salud y seguridad. También se debería tener en consideración cualquier amenaza de seguridad presente en la cercanía de las instalaciones, por ejemplo, fugas de agua de otras áreas.

NCh2777

Se deberían considerar los controles siguientes:

- a) Las instalaciones claves se deberían ubicar de modo de evitar el acceso del público.
- b) Los edificios deberían ser discretos y dar una mínima indicación de su propósito, sin signos obvios que identifiquen la presencia de actividades de procesamiento de información, en el exterior e interior del mismo.
- c) Las funciones y equipos de apoyo, por ejemplo, fotocopadoras, máquinas de fax, se deberían situar apropiadamente dentro del área segura para evitar la petición de acceso a ellos, lo que podría comprometer la información.
- d) Las puertas y ventanas se deberían cerrar con llave cuando estén sin personas y para las ventanas se debería considerar una protección externa, particularmente cuando están en el primer piso.
- e) Se deberían colocar sistemas apropiados de detección de intrusos, instalarlos con normas profesionales y probarlos regularmente, para cubrir todas las puertas externas y ventanas accesibles. Las áreas desocupadas deberían tener alarmas todo el tiempo. También se debería proveer esta cobertura en otras áreas, por ejemplo, salas de computadores y comunicaciones.
- f) Las instalaciones de procesamiento de la información gestionadas por la organización se deberían separar físicamente de aquellas gestionadas por terceras partes.
- g) Las guías de teléfonos internos y directorios que identifican ubicaciones de equipos de procesamiento de información sensible, no deberían ser fácilmente accesibles por el público.
- h) Los materiales peligrosos o combustibles se deberían almacenar a una distancia alejada del área segura. Los suministros, tales como los útiles de escritorio no se deberían almacenar dentro de un área segura hasta que sea necesario.
- i) Los equipos y dispositivos de respaldo se deberían situar a una distancia segura para evitar los daños de un desastre del sitio principal.

7.1.4 Trabajo en áreas seguras

Se pueden necesitar controles y guías adicionales para reforzar la seguridad de un área segura. Esto incluye controles para el personal y de terceras partes que trabajan en el área segura, así como a las actividades de terceras partes que se realizan allí. Se deberían considerar los controles siguientes:

- a) El personal debería saber de la existencia de un área segura, o tener conocimientos básicos de las actividades dentro del área, solamente si es necesario.
- b) Se deberían evitar los trabajos no supervisados dentro de un área segura, por razones de seguridad y para prevenir las oportunidades de actividades maliciosas.

- c) Las áreas seguras vacantes se deberían cerrar físicamente con llave y se deberían revisar periódicamente.
- d) Se debería otorgar acceso restringido al personal de los servicios de apoyo de terceras partes, a las áreas seguras o a las instalaciones de procesamiento de información sensible y solamente cuando sea necesario. Este acceso se debería autorizar y monitorear. Pueden ser necesarias barreras adicionales y perímetros de control de acceso físico, entre áreas con diferentes requisitos de seguridad internas en el perímetro de seguridad.
- e) No se deberían permitir los equipos de video, audio, fotografía u otros equipos de grabación, a menos que sea autorizado.

7.1.5 Áreas de carga y entrega aisladas

Se deberían controlar las áreas de carga y entrega y, si es posible, aisladas de los equipos de procesamiento de información, para evitar el acceso no autorizado. Los requisitos de seguridad de tales áreas se deberían determinar por la evaluación del riesgo. Se deberían considerar los controles siguientes:

- a) El acceso al área de suministros desde el exterior del edificio se debería restringir al personal identificado y autorizado.
- b) El área de suministros se debería designar de modo que las mercaderías se puedan descargar sin dar acceso al personal a otras partes del edificio.
- c) Las puertas externas del área de suministros se deberían asegurar cuando las puertas internas se abran.
- d) El material entrante se debería inspeccionar de potenciales peligros [ver 7.2.1 d)] antes de que se traslade desde el área de suministros al punto de uso.
- e) El material entrante se debería registrar, si es apropiado (ver 5.1), en la entrada al sitio.

7.2 Seguridad de los equipos

Objetivo: Prevenir pérdidas, daños o compromiso de los bienes e interrupción de las actividades del negocio.

Se deberían proteger físicamente los equipos de las amenazas de seguridad y riesgos del ambiente externo. Es necesaria la protección de los equipos (que incluye el que se usa fuera del sitio) para reducir el riesgo de acceso no autorizado a datos y para prevenir la pérdida o daño. Esto también debería considerar la ubicación de los equipos y la eliminación de ítems en desuso. Se pueden necesitar controles especiales para protegerlos de riesgos o accesos no autorizados, y salvaguardar las instalaciones de apoyo, tales como el suministro eléctrico y la infraestructura de cables.

7.2.1 Ubicación y protección de los equipos

Los equipos se deberían ubicar en un lugar particular o protegerlos para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado. Se deberían considerar los controles siguientes:

- a) Los equipos se deberían ubicar de tal forma de minimizar el acceso innecesario a las áreas de trabajo.
- b) Las instalaciones de almacenaje y procesamiento de información, donde se manipulan datos sensibles se deberían instalar de modo de reducir el riesgo de descuidos durante su uso.
- c) Los ítemes que requieren protección especial se deberían aislar de modo de reducir el nivel general de protección necesaria.
- d) Se deberían adoptar controles que minimicen el riesgo de amenazas potenciales, las que incluyen:
 - d.1) hurto;
 - d.2) fuego;
 - d.3) explosivos;
 - d.4) humo;
 - d.5) agua (o falla del suministro);
 - d.6) polvo;
 - d.7) vibración;
 - d.8) efectos químicos;
 - d.9) interferencia en el suministro eléctrico;
 - d.10) radiación electromagnética.
- e) La organización debería considerar en su política lo que respecta a comer, beber y fumar en la proximidad de las instalaciones de procesamiento de información.
- f) Se deberían monitorear las condiciones ambientales para determinar las condiciones que podrían afectar adversamente la operación de las instalaciones de procesamiento de información.

- g) Se debería considerar el uso de métodos de protección especiales, tales como membranas para teclados, para equipos en ambientes industriales.
- h) Se debería considerar el impacto de la ocurrencia de un desastre en las cercanías de las instalaciones, por ejemplo, fuego en las cercanías del edificio, fuga de agua desde el cielo del edificio o en los pisos bajo el nivel de la tierra o una explosión en la calle.

7.2.2 Suministro de energía eléctrica

Los equipos se deberían proteger de fallas de suministro de energía y otras anomalías eléctricas. Se debería proveer un suministro de energía eléctrica adecuado, que esté conforme con las especificaciones del fabricante.

Las opciones para lograr la continuidad del suministro de energía eléctrica incluyen:

- a) alimentación múltiple para prevenir la falla de un solo punto en el suministro de energía eléctrica;
- b) suministro ininterrumpido de energía eléctrica (UPS);
- c) generador de respaldo.

Se recomienda una UPS para apoyar el cierre ordenado del sistema o para que continúe en operación, en equipos que apoyan las operaciones críticas del negocio. Los planes de contingencia deberían cubrir la acción a tomar cuando falle la UPS. Los equipos UPS se debería verificar regularmente para asegurar su adecuada capacidad y probarlos de acuerdo con las recomendaciones del fabricante.

Se debería considerar un generador de respaldo si el procesamiento debe continuar aún en caso de una falla prolongada del suministro de energía eléctrica. Si hay generadores instalados, se deberían probar regularmente de acuerdo con las instrucciones del fabricante. Se debería disponer de un adecuado suministro de combustible, para asegurar que el generador puede trabajar por un período prolongado.

Además, se debería colocar un interruptor de energía eléctrica de emergencia cerca de la salida de emergencia de la sala equipos, para facilitar un rápido corte de la energía eléctrica en caso de una emergencia. Se debería proveer iluminación de emergencia en caso de falla del suministro de energía eléctrica principal. Se debería aplicar protección contra rayos en todos los edificios y los filtros de protección contra rayos deberían ser aptos para todas las líneas externas de comunicaciones.

7.2.3 Seguridad del cableado

Los cables de energía eléctrica y telecomunicaciones que llevan datos o servicios de apoyo a la información, se deberían proteger de interceptaciones o daños. Se deberían considerar los controles siguientes:

- a) Las líneas de energía eléctrica y telecomunicaciones en las instalaciones de procesamiento de información deberían ser subterráneas, cuando sea posible, o sujetas a una protección alternativa adecuada.
- b) El cableado de redes se debería proteger de la interceptación o daños de personas no autorizadas, por ejemplo, usando canaletas portacables, o evitando rutas que pasen por áreas públicas.
- c) Los cables de energía eléctrica se deberían separar de los cables de comunicación para evitar interferencias.
- d) En los sistemas sensibles y críticos además de los controles en consideración, incluir:
 - d.1) La instalación de canaletas portacables blindadas y salas o cajas con llave en los puntos de inspección y terminación;
 - d.2) El uso de rutas o dispositivos de transmisión alternativos;
 - d.3) El uso de cables de fibra óptica;
 - d.4) Retirar los dispositivos no autorizados que estén junto a los cables.

7.2.4 Mantenimiento de los equipos

Los equipos se deberían mantener correctamente para asegurar su integridad y disponibilidad continua. Se deberían considerar los controles siguientes:

- a) Los equipos deberían tener su mantenimiento de acuerdo con las especificaciones e intervalos de servicios recomendados por el proveedor.
- b) Solamente el personal de mantenimiento autorizado debería realizar las reparaciones y servicios de los equipos.
- c) Se deberían guardar los registros de todas las fallas sospechosas o reales y de los mantenimientos correctivos y preventivos.
- d) Se deberían tomar en cuenta los controles apropiados cuando se envían equipos de las instalaciones para mantenimiento, (ver también 7.2.6 respecto a la anulación, borrado, y sobre-escritura de datos). Se deberían cumplir todos los requisitos impuestos por las políticas de seguridad.

7.2.5 Seguridad de los equipos fuera de la organización

Independiente de la propiedad, la dirección debería autorizar si es pertinente el uso fuera de la organización de cualquier equipo para el procesamiento de información. La seguridad debería ser equivalente a la que tienen los equipos cuando está en el sitio de uso normal, para el mismo propósito, tomando en cuenta los riesgos de trabajar externamente a las instalaciones de la organización. Los equipos de procesamiento de información incluyen todas las formas de computadores personales, organizadores, teléfonos móviles, papel u otra forma que se usa para trabajar en el hogar o que se transporta desde el sitio normal de trabajo a otro lugar. Se deberían considerar las guías siguientes:

- a) Los equipos y los dispositivos que se ocupan fuera de las instalaciones de la organización no se deberían dejar desatendidos en lugares públicos. Los computadores portátiles se deberían llevar en un bolso de mano y disimulados durante un viaje, cuando sea posible.
- b) Las instrucciones de protección del fabricante de los equipos se deberían observar todo el tiempo, por ejemplo, la protección a la exposición de campos electromagnéticos intensos.
- c) Los controles del trabajo realizado en el hogar se deberían determinar mediante la evaluación del riesgo y aplicar los controles adecuados cuando sea apropiado, por ejemplo, gabinetes de archivo con llaves, política de escritorio limpio y controles de acceso a los computadores.
- d) Se debería tener la cobertura de seguros adecuados para proteger los equipos fuera del sitio normal.

Los riesgos de la seguridad, por ejemplo, de daño, robo y escucha prohibida, pueden variar considerablemente entre ubicaciones y se debería tomar en cuenta en la determinación de los controles más apropiados. En 9.8.1 se puede encontrar más información con respecto a otros aspectos de protección de equipos móviles.

7.2.6 Seguridad en la eliminación de ítemes en desuso o reuso de equipos

La información se puede comprometer debido a un descuido en la eliminación de ítemes en desuso o a un reuso de equipos (ver también 8.6.4). Los dispositivos de almacenamiento que contienen información sensible se deberían destruir físicamente o sobrescribir en forma segura usando una función de borrado estandarizado.

Todos los ítemes de los equipos que contienen dispositivos de almacenamiento, por ejemplo, discos duros fijos, se deberían revisar para asegurar que cualquier dato sensible y licencia de software se haya sacado o sobrescrito antes de la eliminación. Los dispositivos de almacenamiento que contienen datos sensibles pueden necesitar una evaluación del riesgo, para determinar si los ítemes se deberían destruir, reparar o descartar.

7.3 Controles generales

Objetivo: Prevenir que se comprometa o se robe la información y equipos de procesamiento de información.

La información y los equipos de procesamiento de información se deberían proteger de la divulgación, modificación o del robo por personas no autorizadas, y los controles se deberían realizar en el sitio para minimizar la pérdida o daño.

En 8.6.3 se consideran los procedimientos de manipulación y almacenamiento.

7.3.1 Política de escritorio limpio y pantalla limpia

Las organizaciones deberían considerar la adopción de la política de escritorio limpio, para los papeles y dispositivos removibles de almacenamiento y una política de pantalla limpia, para los equipos de procesamiento de información con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante y fuera de las horas normales de trabajo. La política debería tomar en cuenta las clasificaciones de la 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 es probable que se dañe o destruya por un desastre tal como fuego, inundación o explosión.

Se deberían considerar los controles siguientes:

- a) Cuando sea apropiado, el papel y los dispositivos del computador, cuando no se usen, se deberían almacenar en gabinetes adecuados con llave y/o o en otras formas de muebles con seguridad especialmente fuera de las horas de trabajo.
- b) La información crítica o sensible del negocio, se debería colocar alejada del sitio con llave, (idealmente en una caja de seguridad o gabinete resistente al fuego) cuando no se necesite, especialmente cuando la oficina esté desocupada.
- c) Los computadores personales, los terminales de computadores y las impresoras no se deberían dejar con la sesión abierta, cuando estén desatendidos y cuando no se usen se deberían proteger con llaves con clave, contraseña y otros controles.
- d) Los puntos de correo salientes y entrantes, máquinas de fax y telex no atendidos se deberían proteger.
- e) Las fotocopadoras se deberían tener con llave (o protegidas de alguna manera de los usuarios no autorizados) fuera de las horas normales de trabajo.
- f) La información clasificada o sensible, cuando se imprima se debería retirar inmediatamente de las impresoras.

7.3.2 Remoción de bienes

Los equipos, la información o software no se deberían ocupar fuera del sitio sin autorización. Cuando sea necesario y apropiado, los equipos deberían quedar con las sesiones cerradas y cuando vuelva a su lugar se deberían reiniciar las sesiones. Se debería realizar la revisión de los puestos de trabajo para detectar la remoción no autorizada de algún inmueble. Se les debería hacer conciencia a las personas que se realizarán revisiones a los puestos de trabajo.

8 Gestión de las operaciones y de las comunicaciones

8.1 Responsabilidades y procedimientos de las operaciones

Objetivo: Asegurar la correcta y segura operación de los equipos de procesamiento de información.

Se deberían establecer las responsabilidades y los procedimientos para la gestión y operación de todos los equipos de procesamiento de información. Esto incluye el desarrollo de instrucciones de operación apropiadas y procedimientos de respuesta a incidentes.

Se debería implementar la separación de obligaciones (ver 8.1.4), cuando sea apropiado, para reducir el riesgo de negligencia o mal uso deliberado del sistema.

8.1.1 Procedimientos de operación documentados

Los procedimientos de operación identificados por la política de seguridad, se deberían documentar y mantener. Los procedimientos de operación se deberían tratar como documentos formales y los cambios deberían ser autorizados por la dirección.

Los procedimientos deberían especificar las instrucciones para una ejecución detallada de cada trabajo, incluyendo:

- a) procesamiento y manipulación detallada de la información;
- b) requerimientos de programación de horarios que incluyan las interdependencias con otros sistemas, el comienzo más temprano y el término más tardío del trabajo;
- c) instrucciones para manipular errores u otras condiciones excepcionales, que pueden aparecer durante la ejecución del trabajo, incluyendo restricciones en el uso de los equipos del sistema (ver 9.5.5);
- d) contactos de apoyo en el evento de dificultades técnicas u operacionales inesperadas;

- e) instrucciones de manipulación de salidas especiales, tales como el uso de útiles de librería especiales o la gestión de una salida confidencial, incluyendo procedimientos de eliminación segura de los trabajos malos, en desuso, de salida;
- f) procedimientos de reinicio del sistema y de recuperación a ser utilizados en el evento de que el sistema falle.

Los procedimientos documentados se deberían preparar también para las actividades de administración interna del sistema, asociados con las instalaciones de comunicación y de procesamiento de información, tal como el reinicio de un computador o los procedimientos de cierre, respaldo, mantenimiento de los equipos, sala de computadores y gestión de manipulación del correo y sistema de seguridad.

8.1.2 Control de cambio de operación

Se deberían controlar los cambios de instalaciones y sistemas de procesamiento de información. El control inadecuado de cambios de sistemas e instalaciones de procesamiento de información es una causa común de fallas de seguridad. Las responsabilidades y procedimientos formales de gestión deberían estar en el sitio para asegurar el control satisfactorio de todos los cambios a los equipos, software o procedimientos. Los programas de operación deberían estar sujetos a un control estricto de cambio. Cuando los programas se cambian se debería guardar un registro de auditoría que contenga toda la información pertinente. Los cambios de ambiente operacional pueden impactar las aplicaciones. Donde quiera que sea práctico, se deberían integrar los procedimientos de control de cambios (ver también 10.5.1). En particular se deberían considerar los controles siguientes:

- a) identificación y registro de cambios significativos;
- b) evaluación del impacto potencial de tales cambios;
- c) procedimiento formal de aprobación de los cambios propuestos;
- d) comunicación de los detalles de los cambios a todas las personas que sea pertinente;
- e) procedimientos que identifiquen las responsabilidades para recuperar la condición inicial y abortar los cambios no exitosos.

8.1.3 Procedimientos de gestión de incidentes

Se deberían establecer los procedimientos y las responsabilidades de gestión de incidentes, para asegurar una rápida, efectiva y metódica respuesta a la seguridad de incidentes (ver también 6.3.1). Se deberían considerar los controles siguientes:

- a) Establecer los procedimientos para cubrir todos los tipos de incidentes potenciales de seguridad, incluyendo:
 - a.1) fallas del sistema de información y pérdida de servicio;
 - a.2) denegación del servicio;
 - a.3) errores que resultan de datos inexactos e incompletos del negocio;
 - a.4) violación de la confidencialidad.
- b) Además de los planes normales de contingencia (diseñados para recuperar los sistemas o servicios tan rápido como sea posible), los procedimientos deberían cubrir (ver también 6.3.4):
 - b.1) el análisis e identificación de la causa del incidente;
 - b.2) si es necesario, planificación e implementación de soluciones para evitar que vuelva a ocurrir;
 - b.3) reunir las pruebas de auditoría y evidencias similares;
 - b.4) comunicación con los afectados o involucrados con la recuperación del incidente;
 - b.5) informar la acción a la autoridad apropiada.
- c) Se deberían reunir y dejar guardadas las pruebas de auditoría y evidencias similares (ver 12.1.7), apropiadas para:
 - c.1) el análisis interno del problema;
 - c.2) el uso como evidencia en relación a una potencial violación del contrato, violación de los requisitos regulatorios o en el evento de un procesamiento judicial, por ejemplo, por mal uso de los computadores o por la aplicación de la legislación de protección de datos;
 - c.3) la negociación de compensación de parte de los proveedores de software y servicios.

- d) Se deberían controlar formalmente y cuidadosamente las acciones para recuperar el sistema de las fallas y violaciones a la seguridad. Los procedimientos deberían asegurar que:
 - d.1) sólo el personal autorizado y claramente identificado tenga acceso a los datos y sistemas existentes (ver también 4.2.2 para el acceso de terceras partes);
 - d.2) todas las acciones de emergencia que se tomen se documenten en detalle;
 - d.3) una acción de emergencia sea informada a la dirección y revisada de una manera metódica;
 - d.4) la integridad de los sistemas y controles del negocio sea confirmada con un retardo mínimo.

8.1.4 Separación de responsabilidades

La separación de las responsabilidades es un método para reducir el riesgo de un mal uso deliberado o accidental del sistema. Se debería considerar la separación de la gestión o ejecución de ciertas responsabilidades o áreas de responsabilidad, con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de información o servicios.

Las organizaciones pequeñas pueden encontrar este método difícil de lograr, pero el principio se debería aplicar tanto como sea posible y práctico. Cuando sea difícil realizar una separación, se deberían considerar otros controles tales como el monitoreo de actividades, pruebas de auditorías y supervisión de la gestión. Es importante que las auditorías de seguridad permanezcan independientes.

Se debería cuidar que ninguna persona por sí sola pueda perpetrar fraudes en áreas de responsabilidad individual sin que sea detectada. Se debería separar el inicio de un evento, de su autorización. Se deberían considerar los controles siguientes:

- a) Es importante separar las actividades que requieren confabulación para realizar un fraude, por ejemplo, la emisión de una orden de compra y la verificación de que las mercaderías se hayan recibido.
- b) Si hay un peligro de confabulación, entonces los controles necesitan ser ideados de modo que sea necesario que dos o más personas estén involucradas, con lo cual se baja la posibilidad de conspiración.

8.1.5 Separación de las instalaciones de desarrollo y operaciones

Es importante la separación entre las instalaciones de desarrollo, prueba y operación para lograr la separación de roles involucrados. Se deberían definir y documentar las reglas para la transferencia de software del estado de desarrollo al de operación.

Las actividades de desarrollo y de prueba pueden causar serios problemas, por ejemplo, la modificación indeseada de archivos o del ambiente del sistema o falla del sistema. Se debería considerar el nivel de separación que sea necesario entre los ambientes de operación, de prueba y de desarrollo, para prevenir problemas de operación. Una separación similar también se debería implementar entre las funciones de desarrollo y prueba. En este caso, hay una necesidad de mantener un ambiente estable y conocido en el cual realizar pruebas significativas y prevenir el acceso inadecuado a desarrolladores.

Cuando el personal de desarrollo y de prueba tiene acceso al sistema en operación y a su información, ellos pueden introducir códigos no probados y no autorizados o alterar los datos de operación. En algunos sistemas, esta capacidad podría ser mal usada para cometer fraudes o introducir códigos maliciosos o no probados. Los códigos maliciosos o no probados pueden producir serios problemas de operación. Los desarrolladores y probadores también plantean una amenaza a la confidencialidad de la información de operación.

Las actividades de desarrollo y de prueba pueden causar cambios no intencionales al software y a la información si ellos comparten el mismo ambiente computacional. Por lo tanto es deseable la separación de las instalaciones de desarrollo, prueba y operación, para reducir el riesgo de un cambio accidental o acceso no autorizado al software de operación y a los datos del negocio. Se deberían considerar los controles siguientes:

- a) El software de desarrollo y el operacional se deberían ejecutar, cuando sea posible, en diferentes procesadores de computador o en diferentes dominios o directorios.
- b) Las actividades de desarrollo y prueba se deberían separar tanto como sea posible.
- c) Los compiladores, editores y otros equipos del sistema deberían ser inaccesibles desde los sistemas operacionales cuando no sea necesario.
- d) Diferentes procedimientos de registro se deberían usar para las operaciones y pruebas del sistema, para reducir el riesgo de error. Se debería incentivar a los usuarios a usar diferentes contraseñas para estos sistemas, y los menús deberían mostrar mensajes de identificación apropiados.
- e) El personal de desarrollo debería tener acceso a las contraseñas de operación sólo para el apoyo de los sistemas en operación, cuando los controles estén operativos para la revisión de las contraseñas. Los controles deberían asegurar que tales contraseñas se cambien después de su uso.

8.1.6 Gestión externa de las instalaciones

El uso de personal externo para gestionar las instalaciones de procesamiento de información puede introducir una potencial exposición de la seguridad, tal como la posibilidad de comprometer, dañar, o perder los datos en el sitio del personal externo. Estos riesgos se deberían identificar por adelantado, y se deberían acordar los controles apropiados con el personal externo e incorporarlos en el contrato (ver también 4.2.2 y 4.3 para la guía de los contratos de terceras partes que involucren el acceso a las instalaciones de la organización y contratos de externalización).

Se debería consignar que se incluyan las materias siguientes:

- a) identificar las aplicaciones sensibles o críticas, las que sean mejor mantener internamente;
- b) obtener la aprobación de los dueños de la aplicación del negocio;
- c) implicancias de los planes de continuidad del negocio;
- d) normas de seguridad específicas y los procesos para medir su cumplimiento;
- e) asignación de responsabilidades y procedimientos para monitorear efectivamente todas las actividades pertinentes de seguridad;
- f) responsabilidades y procedimientos para informar y gestionar los incidentes de seguridad (ver 8.1.3).

8.2 Aceptación y planificación del sistema

Objetivo: Minimizar el riesgo de fallas de los sistemas.

Es necesario la preparación y planificación por adelantado para asegurar la disponibilidad de recursos y capacidad adecuada.

Se deberían hacer proyecciones de los requisitos futuros de capacidad, para reducir el riesgo de sobrecarga.

Se deberían establecer los requisitos de operación de los nuevos sistemas, documentar y probar antes de su aceptación y uso.

8.2.1 Planificación de la capacidad

Las demandas de capacidad de proceso se deberían monitorear y hacer proyecciones de los requerimientos futuros para asegurar que esté disponible una adecuada capacidad de proceso y almacenamiento. Estas proyecciones deberían tomar en cuenta los nuevos negocios y los requisitos del sistema, la tendencia actual y proyectada en el procesamiento de la información de la organización.

Los computadores principales requieren atención particular, debido al alto costo y tiempo para obtener un aumento de capacidad. Los directivos encargados de los computadores principales de servicios deberían monitorear la utilización de los recursos claves del sistema, incluyendo procesadores, almacenamiento principal, almacenamiento en archivo, impresoras y otros dispositivos de salida, y sistemas de comunicaciones. Ellos deberían identificar las tendencias en el uso de estos, particularmente en relación a las aplicaciones del negocio o herramientas del sistema de gestión de la información.

Los directivos deberían usar esta información para identificar y evitar potenciales cuellos de botella que puedan presentar una amenaza a la seguridad del sistema o a los servicios del usuario y planificar una acción de solución apropiada.

8.2.2 Aceptación del sistema

Se deberían establecer los criterios de aceptación de los nuevos sistemas de información, actualizaciones, nuevas versiones y de las pruebas apropiadas a realizar al sistema antes de la aceptación. Los directivos deberían asegurar que los requisitos y criterios de aceptación de los nuevos sistemas sean definidos claramente, acordados, documentados y probados. Se deberían considerar los controles siguientes:

- a) requisitos de desempeño y capacidad del computador;
- b) procedimientos de reinicio, de recuperación por error y planes de contingencia;
- c) preparación y prueba de los procedimientos de operación rutinarios según las normas definidas;
- d) acordar un conjunto de controles de seguridad en el sitio;
- e) procedimientos manuales efectivos;
- f) configuraciones de continuidad del negocio, como lo requerido en 11.1;
- g) evidencia de que la instalación de los nuevos sistemas no afectarán adversamente los sistemas existentes, particularmente en los tiempos de máximo procesamiento, tales como fines de mes;
- h) evidencia de que se ha tomado en consideración el efecto del nuevo sistema en toda la seguridad de la organización;
- i) entrenamiento en la operación o uso de los nuevos sistemas.

Para desarrollos nuevos y más extensos, se debería consultar a los usuarios y las funciones de operación en todas las etapas de desarrollo del proceso, para asegurar la eficiencia operacional del diseño del sistema propuesto. Se deberían realizar las pruebas apropiadas para confirmar que todos los criterios de aceptación se satisfagan totalmente.

8.3 Protección contra el software malicioso

Objetivo: Proteger la integridad del software y de la información.

Se requiere tomar precauciones para prevenir y detectar la introducción de software malicioso.

Las instalaciones de procesamiento de información y el software son vulnerables a la introducción de software malicioso, tal como virus computacional, worms, troyanos (ver también 10.5.4) y bombas lógicas. Los usuarios deberían tener conciencia de los peligros del software malicioso o no autorizado, y los directivos deberían, cuando sea apropiado, agregar controles especiales para detectar o prevenir su introducción. En particular es esencial que se tomen precauciones para detectar y prevenir los virus computacionales en los computadores personales.

8.3.1 Controles contra el software malicioso

Se deberían implementar controles y procedimientos apropiados para la sensibilización de prevención y detección contra el software malicioso. La protección contra el software malicioso se debería basar en la sensibilización sobre seguridad, sistemas adecuados de acceso y controles de gestión de cambios. Se deberían considerar los controles siguientes:

- a) una política formal que exija el cumplimiento con las licencias de software y prohibir el uso de software no autorizado (ver 12.1.2.2);
- b) una política formal para protegerse de los riesgos asociados con la obtención vía redes externas de archivos y software, o por otros medios, indicando qué medidas de protección se deberían tomar (ver también 10.5, especialmente 10.5.4 y 10.5.5);
- c) instalación y actualización permanente de software antivirus de detección y reparación, para examinar computadores y dispositivos, ya sea como un control preventivo o como rutina básica;
- d) revisiones regulares de comportamiento del software y datos que contienen los sistemas de apoyo a los procesos críticos del negocio. Se debería investigar formalmente la presencia de cualquier archivo no aprobado o correcciones no autorizadas;
- e) verificación de virus antes de usar cualquier archivo en un dispositivo electrónico de origen incierto o no autorizado, o archivos recibidos de redes no confiables;
- f) verificación de software maliciosos antes usar cualquier archivo adjunto de correo electrónico y descargas de archivos. Esta verificación se puede realizar en diferentes lugares, por ejemplo, en el servidor de correo electrónico, computadores de escritorio o cuando se entre a la red de la organización;

- g) responsabilidades y procedimientos de gestión para tratar la protección contra virus en los sistemas, entrenamiento de su uso, informe y recuperación de ataques de virus (ver 6.3 y 8.1.3);
- h) planes apropiados de continuidad del negocio para la recuperación por ataques de virus, incluyendo todos los respaldos de datos y software necesarios y disposiciones de recuperación (ver cláusula 11);
- i) procedimientos para verificar toda la información relacionada con el software malicioso y asegurar que los boletines de advertencias sean exactos e informativos. Los directivos deberían asegurar cuáles son las fuentes calificadas, por ejemplo, revistas de prestigio, sitios de internet confiables o proveedores de software antivirus, para diferenciar entre bromas y virus reales. El personal debería tener conciencia del problema de las bromas y qué hacer al recibo de ellas.

Estos controles son especialmente importantes para redes de servidores de apoyo a gran número de estaciones de trabajo.

8.4 Administración interna

Objetivo: Mantener la integridad y disponibilidad del procesamiento de información y de los servicios de comunicación.

Se deberían establecer los procedimientos de rutina para realizar la estrategia de respaldo acordada (ver 11.1), tomando copias de respaldo de los datos y ensayando su recuperación oportunamente, registrando los eventos y fallas y cuando sea apropiado, monitoreando el ambiente de los equipos.

8.4.1 Respaldo de la información

Se deberían tomar regularmente copias de respaldo de la información y software esencial del negocio. Se deberían proveer las instalaciones adecuadas de respaldo para asegurar que toda la información y el software esencial del negocio se pueda recuperar después de un desastre o una falla de algún dispositivo. Las configuraciones de respaldo para los sistemas individuales se deberían probar regularmente para asegurar que ellas cumplen con los requisitos de los planes de continuidad del negocio (ver cláusula 11). Se deberían considerar los controles siguientes:

- a) Almacenar en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento, esta ubicación debería estar a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. Al menos tres generaciones o ciclos de información de respaldo se deberían guardar en aplicaciones importantes del negocio.

NCh2777

- b) A la información de respaldo se le debería dar un apropiado nivel de protección física y del medio (ver cláusula 7), consistente con las normas aplicadas en el sitio principal. Los controles aplicados a los dispositivos en el sitio principal se deberían extender para cubrir el sitio de respaldo.
- c) Los dispositivos de respaldo se deberían probar regularmente, cuando sea práctico, para asegurar que ellos pueden ser de uso confiable en una emergencia cuando sea necesario.
- d) Los procedimientos de restablecimiento se deberían revisar y probar regularmente para asegurar que ellos son efectivos y que se pueden completar dentro del tiempo asignado a los procedimientos de recuperación de la operación.

Se debería determinar el período de retención de la información esencial del negocio, y también cualquier requisito para archivar copias que estén permanentemente guardadas (ver 12.1.3).

8.4.2 Registros del operador

El personal de operaciones debería mantener un registro de sus actividades. Los registros deberían incluir, cuando sea apropiado:

- a) hora de inicio y término del sistema;
- b) errores del sistema y acciones correctivas tomadas;
- c) confirmación de la manipulación correcta de los archivos de datos y salidas del computador;
- d) el nombre de la persona que hace el registro de entrada.

Los registros del operador deberían estar sujetos a revisiones independientes y regulares de los procedimientos de operación.

8.4.3 Registro de falla

Se deberían informar las fallas y la acción correctiva tomada. Se deberían registrar las fallas informadas por los usuarios en relación a problemas con los sistemas de procesamiento de información o comunicaciones. Deberían existir reglas claras para la manipulación de informes de fallas, incluyendo:

- a) revisión de registros de falla para asegurar que éstas se hayan resuelto satisfactoriamente;
- b) revisión de medidas correctivas para asegurar que los controles no se hayan comprometido y que la acción tomada esté totalmente autorizada.

8.5 Gestión de red

Objetivo: Asegurar la salvaguardia de la información en las redes y protección de la infraestructura de apoyo.

Requiere atención la gestión de seguridad de las redes que pueden extender los límites de la organización.

También se pueden necesitar controles adicionales para proteger los datos sensibles que pasan por redes públicas.

8.5.1 Controles de redes

Para lograr y mantener la seguridad en redes de computadores es necesario una variedad de controles. Los administradores de redes deberían implementar controles para resguardar la seguridad de los datos en las redes, y la protección de los accesos no autorizados a los servicios conectados. Se deberían considerar en particular los controles siguientes:

- a) La responsabilidad operacional de las redes se debería separar de las operaciones del computador cuando sea apropiado (ver 8.1.4).
- b) Se deberían establecer las responsabilidades y procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios.
- c) Si es necesario, se deberían establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan por las redes públicas, y para proteger los sistemas conectados (ver 9.4 y 10.3). Para mantener la disponibilidad de los servicios de la red y de los computadores conectados pueden ser necesarios controles especiales.
- d) Las actividades de gestión deberían estar coordinadas para optimizar el servicio del negocio y asegurar que los controles sean consistentemente aplicados a toda la infraestructura de procesamiento de la información.

8.6 Seguridad y manipulación de dispositivos

Objetivo: Prevenir daños a los bienes e interrupciones a las actividades del negocio. Los dispositivos se deberían controlar y proteger físicamente.

Se deberían establecer los procedimientos apropiados de operación para proteger de daños, robos y acceso no autorizado a los documentos, dispositivos computacionales (cintas, discos, cassettes), datos de entrada y salida y a la documentación del sistema.

8.6.1 Gestión de dispositivos removibles de computadores

Deberían existir procedimientos para la gestión de dispositivos computacionales, removibles, tales como cintas, discos, cassettes e informes impresos. Se deberían considerar los controles siguientes:

- a) Se deberían borrar los contenidos previos de cualquier dispositivo reutilizable que se retire de la organización, si ya no se necesita.
- b) Se debería necesitar autorización para todos los dispositivos que se retiren de la organización y conservar un registro de tales retiros para mantener una auditoría de seguimiento (ver 8.7.2).
- c) Se deberían almacenar todos los dispositivos en un lugar y ambiente seguro, de acuerdo con las especificaciones del fabricante.

Todos los procedimientos y niveles de autorización deberían estar claramente documentados.

8.6.2 Eliminación de dispositivos en desuso

Los dispositivos se deberían eliminar sin riesgos ni accidentes cuando no se necesiten más. La información sensible se podría fugar a personas externas a través de la eliminación descuidada de dispositivos en desuso. Para minimizar este riesgo se deberían establecer los procedimientos formales para la eliminación segura de los dispositivos en desuso. Se deberían considerar los controles siguientes:

- a) Los dispositivos que contienen información sensible se deberían almacenar y desechar sin riesgos ni accidentes, por ejemplo, por incineración o trituración, o vaciado de los datos mediante otra aplicación dentro de la organización.
- b) La siguiente lista identifica los ítemes en desuso que podrían necesitar una eliminación segura:
 - b.1) documentos de papel;
 - b.2) grabaciones de voz u otra;
 - b.3) papel calco;
 - b.4) informes de salida;
 - b.5) cintas de impresora de un solo uso;
 - b.6) cintas magnéticas;
 - b.7) discos removibles o cassettes;

- b.8) dispositivos de almacenamiento óptico (todas las formas, incluyendo los medios de distribución de todos los fabricantes de software);
 - b.9) listados de programas;
 - b.10) datos de prueba;
 - b.11) documentación del sistema.
- c) Puede ser más fácil juntar y disponer de todos los ítemes de los dispositivos y deshacerse sin riesgos, más que intentar separar los ítemes sensibles.
 - d) Muchas organizaciones ofrecen los servicios de juntar y eliminar los papeles, dispositivos y equipos en desuso. Se debería tener cuidado en seleccionar el personal externo adecuado con experiencia y controles apropiados.
 - e) La eliminación de ítemes sensibles en desuso se debería registrar, cuando sea posible, con el fin de mantener una auditoría de seguimiento.

Cuando se acumulan dispositivos en desuso, se debería tener en consideración el efecto agregado, los que podrían causar una gran cantidad de información no clasificada y que puede llegar a ser más sensible que una cantidad pequeña de información clasificada.

8.6.3 Procedimientos de manipulación de la información

Se deberían establecer los procedimientos para la manipulación y almacenamiento de la información con el fin de proteger tal información de una divulgación no autorizada o mal uso. Los procedimientos para la manipulación de la información se deberían diseñar de acuerdo con su clasificación (ver 5.2), en documentos, sistemas computacionales, redes, computadores móviles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedios, instalaciones y servicios postales, uso de máquinas de fax y cualquier otro ítem sensible, por ejemplo, cheques en blancos, facturas. Se deberían considerar los controles siguientes (ver también 5.2 y 8.7.2):

- a) manipulación y etiquetado de todos los dispositivos [ver también 8.7.2 a)];
- b) restricciones de acceso para identificar al personal no autorizado;
- c) mantenimiento de un registro formal de los receptores de datos autorizados;
- d) aseguramiento de que los datos de entrada estén completos, que el procesamiento se complete apropiadamente y que se aplique la validación de la salida;
- e) protección de los datos en la cola de espera de impresión de salida, de acuerdo con su sensibilidad;

NCh2777

- f) almacenamiento de los dispositivos en un ambiente que esté de acuerdo con las especificaciones del fabricante;
- g) mantener la distribución de datos al mínimo;
- h) marcar en forma clara todas las copias de datos para la atención de los receptores autorizados;
- i) revisión de las listas de distribución y listas de receptores autorizados a intervalos regulares.

8.6.4 Seguridad de la documentación de sistema

La documentación de sistema puede contener una variedad de información sensible, por ejemplo, descripciones de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización (ver también 9.1). Los siguientes controles se deberían considerar para proteger del acceso no autorizado a la documentación del sistema.

- a) La documentación del sistema se debería almacenar de manera segura.
- b) La lista de acceso a la documentación del sistema debería ser lo más pequeña posible y autorizada por el dueño de la aplicación.
- c) La documentación del sistema que se mantiene en o se suministra vía una red pública, se debería proteger apropiadamente.

8.7 Intercambios de información y software

Objetivo: Prevenir pérdidas, modificación o mal uso de la información intercambiada entre organizaciones.

Los intercambios de información y software entre organizaciones se debería controlar y hacer cumplir con una legislación pertinente (ver cláusula 12).

Los intercambios se deberían incluir en los acuerdos base. Se deberían establecer los procedimientos y normas para proteger los dispositivos y la información en tránsito. Se deberían considerar los requisitos de los controles y las implicancias en el negocio y en la seguridad, asociadas con el intercambio de datos electrónicos, comercio electrónico y correo electrónico.

8.7.1 Acuerdos de intercambio de información y software

Se deberían establecer los acuerdos para el intercambio (ya sea manual o electrónico) de información y software entre organizaciones, algunos de los cuales pueden ser formales, incluyendo cuando corresponda, los acuerdos de software de resguardo. El contenido de seguridad de tal acuerdo debería reflejar la sensibilidad de la información del negocio involucrada. Los acuerdos en las condiciones de seguridad deberían considerar:

- a) responsabilidades de la gestión para controlar y notificar la transmisión, despacho y recepción;
- b) procedimientos para notificar el envío, transmisión, despacho y recepción;
- c) normas técnicas mínimas para empaquetar y transmitir;
- d) normas de identificación del courier;
- e) responsabilidades y obligaciones en el evento de pérdida de datos;
- f) uso de un sistema de etiquetado para la información sensible o crítica, asegurando que el significado de las etiquetas sea inmediatamente entendido y que la información sea apropiadamente protegida;
- g) la propiedad del software y la información y responsabilidades de protección de los datos, cumplimiento con los derechos de propiedad del software y consideraciones similares (ver 12.1.2 y 12.1.4);
- h) normas técnicas para grabar y leer el software y la información;
- i) cualquier control especial que pueda ser necesario para proteger los ítemes sensibles, tales como claves criptográficas (ver 10.3.5).

8.7.2 Seguridad de los dispositivos en tránsito

La información puede ser vulnerable al acceso no autorizado, mal uso o corrupción durante el transporte físico, por ejemplo cuando se envían dispositivos vía servicio postal o courier. Se deberían aplicar los siguientes controles para salvaguardar los dispositivos computacionales que se están transportando entre sitios.

- a) Se deberían usar courier o transportes confiables. Se debería acordar con la dirección una lista de couriers autorizados y un procedimiento para verificar la identificación de los courier implementados.
- b) El empaquetamiento debería ser suficiente para proteger los contenidos de cualquier probable aparición de daño físico durante el tránsito y de acuerdo con las especificaciones del fabricante.

- c) Se deberían adoptar controles especiales, donde sea necesario, para proteger la información sensible a la divulgación o modificación no autorizada. Por ejemplo incluir:
 - c.1) uso de contenedores con llave;
 - c.2) entrega por mano;
 - c.3) empaque con detección de manipulación no autorizada (que revela cualquier intento de obtener acceso);
 - c.4) en casos excepcionales, dividir el envío en más de una entrega y despacho mediante diferentes rutas;
 - c.5) usar la firma electrónica y la encriptación de confidencialidad, ver 10.3.

8.7.3 Seguridad en el comercio electrónico

El comercio electrónico puede involucrar el uso de intercambio de datos digitales (EDI), correo electrónico y transacciones en línea a través de las redes públicas, tal como internet. El comercio electrónico es vulnerable a varias amenazas de la red que pueden llevar a una actividad fraudulenta, disputa contractual y divulgación o modificación de la información. Se deberían aplicar controles para proteger el comercio electrónico de tales amenazas. Se deberían incluir los siguientes controles para considerar la seguridad en el comercio electrónico.

- a) Autenticación. ¿Qué nivel de confianza debería necesitar el cliente y el comerciante, uno del otro al exigir la identidad?
- b) Autorización. ¿Quién está autorizado para colocar precios, emitir o firmar documentos de comercialización? ¿Cómo conoce esto el socio de la comercialización?
- c) Procesos de propuestas y contratos. ¿Cuáles son los requisitos de confidencialidad, integridad y prueba de despacho y recepción de los documentos claves y de no desconocimiento de los contratos?
- d) Información de precio. ¿Qué nivel de confianza se puede poner en la integridad de la lista de precios publicada y la confidencialidad de los convenios de descuentos sensibles?
- e) Transacciones de solicitud. ¿Cómo es la confidencialidad e integridad de la solicitud, pago y detalles de la dirección de entrega y la confirmación de la recepción?
- f) Verificación. ¿Qué grado de verificación es apropiado para revisar la información de pago suministrada por el cliente?
- g) Pago. ¿Cuál es el medio de pago más apropiado, para protegerse de los fraudes?

h) Manejo de solicitudes. ¿Cuál es la protección necesaria para mantener la confidencialidad e integridad de la información de la solicitud y evitar la pérdida o duplicación de la transacción?

i) Responsabilidad. ¿Quién asume el riesgo de cualquier acto fraudulento?

Se pueden considerar varios de los aspectos anteriores mediante la aplicación de las técnicas criptográficas indicadas en 10.3, tomando en cuenta el cumplimiento de los requisitos legales (ver 12.1, especialmente 12.1.6, legislación relacionada con la criptografía).

Los convenios de comercio electrónico entre socios comerciales se deberían apoyar mediante un acuerdo documentado que someta a ambas partes a los términos de comercialización acordados, incluyendo los detalles de autorización [ver b) anterior]. Pueden ser necesarios otros acuerdos con los proveedores de servicios y redes de valor agregado.

Los sistemas públicos de comercialización deberían divulgar entre los clientes los términos del negocio.

Se debería tener en consideración la resistencia del computador usado para el comercio electrónico para defenderse de los ataques y las implicancias en la seguridad de cualquier red de interconexión necesaria para su implementación (ver 9.4.7).

8.7.4 Seguridad del correo electrónico

8.7.4.1 Riesgos de la seguridad

El correo electrónico se usa para las comunicaciones del negocio, reemplazando las formas tradicionales de comunicación, tales como el telex y la carta. El correo electrónico difiere de las formas tradicionales de comunicación de los negocios, por ejemplo, su velocidad, estructura del mensaje, grado de informalidad y vulnerabilidad a acciones no autorizadas. Se debería tener en consideración la necesidad de controles para reducir los riesgos de la seguridad creados por el correo electrónico. Los riesgos de la seguridad incluyen:

- a) vulnerabilidad de los mensajes, modificaciones o accesos no autorizados o ataques de denegación del servicio;
- b) vulnerabilidad a errores, por ejemplo, direcciones incorrectas o direcciones malas, confiabilidad y disponibilidad del servicio en general;
- c) impacto de un cambio en los dispositivos de comunicación en los procesos de los negocios, por ejemplo, el efecto de aumentar la velocidad de despacho o el efecto de enviar mensajes formales de persona a persona antes que de compañía a compañía;

- d) consideraciones legales, tales como la necesidad potencial de comprobar el origen, despacho, entrega y aceptación;
- e) implicancias de tener la lista de personal publicadas para el acceso externo;
- f) control a usuarios con acceso remoto a las cuentas de correo electrónico.

8.7.4.2 Política para el correo electrónico

Las organizaciones deberían formular una política clara para el uso del correo electrónico, incluyendo:

- a) ataques al correo electrónico, por ejemplo, virus, interceptación;
- b) protección de los archivos adjuntos a los correos electrónicos;
- c) guías de cuándo usar o no el correo electrónico;
- d) responsabilidad de los empleados para no comprometer a la compañía, por ejemplo en el envío de correos electrónicos difamatorios, uso para hostigamientos, compras no autorizadas;
- e) uso de técnicas de criptografía para proteger la confidencialidad e integridad de los mensajes electrónicos (ver 10.3);
- f) conservación de mensajes que, si son almacenados, se podrían utilizar en caso de litigios;
- g) controles adicionales para la verificación de mensajes que no se pueden autenticar.

8.7.5 Seguridad de los sistemas de la oficina electrónica

Se deberían preparar e implementar las políticas y guías para controlar el negocio y los riesgos de seguridad asociados con los sistemas electrónicos de oficina. Estas proveen oportunidades para una diseminación y compartición más rápida de la información del negocio usando una combinación de: documentos, computadores, computadores móviles, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedios, instalaciones y servicios postales y equipos de fax.

Teniendo en consideración la seguridad y las implicancias en los negocios de la interconexión de tales instalaciones, se debería incluir:

- a) vulnerabilidades de la información en los sistemas de oficina, por ejemplo, grabación de llamadas o llamadas en conferencia, confidencialidad de las llamadas, almacenamiento de facsímiles, apertura de correo, distribución de correo;
- b) política y controles apropiados para la administración de compartición de la información, por ejemplo, el uso de un boletín electrónico corporativo (ver 9.1);

- c) exclusión de la categoría de información sensible del negocio, si el sistema no provee un apropiado nivel de protección (ver 5.2);
- d) restricción de acceso a la información diaria a personas seleccionadas, por ejemplo, el personal que trabaja en proyectos sensibles;
- e) la conveniencia o no, del sistema para apoyar las aplicaciones en los negocios, tales como comunicaciones de órdenes o autorizaciones;
- f) categorías del personal, externo o socios del negocio que tienen permitido usar el sistema y las ubicaciones desde las cuales se puede acceder (ver 4.2);
- g) restricción a las instalaciones seleccionadas a las categorías específicas de usuarios;
- h) identificación del estado de los usuarios, por ejemplo, a través de un directorio de empleados de la organización o personal externo, para uso de otros usuarios;
- i) conservación y respaldo de la información mantenida en el sistema (ver 12.1.3 y 8.4.1);
- j) requerimientos y configuraciones de recuperación (ver 11.1).

8.7.6 Sistemas disponibles públicamente

Se debería tener cuidado en proteger la integridad de la información publicada electrónicamente para evitar la modificación no autorizada que podría dañar la reputación de la organización que está publicando la información. La información en un sistema disponible públicamente, por ejemplo, la información en un servidor WEB accesible a través de internet, puede ser necesario que deba cumplir con las leyes, reglas y reglamentos de la jurisdicción en la cual el sistema está ubicado o donde se realiza la comercialización. Debería existir un proceso de autorización formal antes que la información esté disponible públicamente.

El software, datos y otra información que necesita un alto nivel de integridad, se debería proteger mediante mecanismos adecuados, para dejarla accesible en un sistema disponible públicamente, por ejemplo, por medio de la firma electrónica (ver 10.3.3). Los sistemas que publican en forma electrónica, especialmente aquellos que permiten realimentación y un ingreso directo de información, se deberían controlar cuidadosamente de modo que:

- a) la información se obtenga en cumplimiento con la legislación de protección de datos (ver 12.1.4);
- b) la información de entrada y la procesada por el sistema de publicación se procese totalmente y exactamente en forma oportuna;
- c) la información sensible se protegerá durante el proceso de recolección y cuando se almacene;
- d) el acceso al sistema de publicación no permita el acceso involuntario a las redes que están conectadas.

8.7.7 Otras formas de intercambio de información

Los procedimientos y controles deberían estar en el sitio para proteger el intercambio de información mediante el uso de las instalaciones de comunicaciones de voz, fax y video. La información se podría comprometer debido a la falta de conocimiento de la política o de los procedimientos para el uso de tales instalaciones, por ejemplo, la escucha casual de un teléfono móvil en un lugar público, las máquinas contestadoras que son escuchadas casualmente, acceso no autorizado por discado a sistemas de correo de voz o el envío accidental de facsímiles a personas equivocadas usando equipos de fax.

Las operaciones del negocio se podrían interrumpir y la información se podría comprometer si fallan, se sobrecargan o interrumpen las instalaciones de comunicaciones (ver 7.2 y cláusula 11). La información también se podría comprometer si éstas son accesibles por usuarios no autorizados (ver cláusula 9).

Se debería tener una declaración de una política clara de los procedimientos que el personal debería seguir en el uso de las comunicaciones de voz, facsímiles y video. Esto incluiría:

- a) recordar al personal que ellos deberían tomar las precauciones apropiadas, por ejemplo no revelar información sensible, evitando la escucha casual o la interceptación cuando se está haciendo una llamada telefónica, por:
 - a.1) las personas de su vecindad inmediata, particularmente cuando se usan teléfonos móviles;
 - a.2) la interceptación de líneas telefónicas y otras formas de escucha no autorizadas a través de acceso físico a los auriculares de los teléfonos o líneas telefónicas, el uso de receptores de exploración cuando se usan teléfonos móviles análogos;
 - a.3) personas en el terminal receptor;
- b) recordar al personal que ellos no deberían tener conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas;
- c) no dejar mensajes en máquinas contestadoras ya que éstas pueden ser escuchadas por personas no autorizadas, almacenar en sistemas comunitarios o almacenar incorrectamente debido a un discado mal realizado;
- d) recordar al personal los problemas relacionados con el uso de los equipos de fax, a saber:
 - d.1) acceso no autorizado al almacén de mensajes predeterminados para recuperarlos;

- d.2) programación deliberada o accidental de los equipos para enviar mensajes a números específicos;
- d.3) envío de documentos y mensajes a un número equivocado por mal discado o uso de un número almacenado equivocado.

9 Control de acceso

9.1 Requisitos del negocio para el control de acceso

Objetivo: Controlar el acceso a la información.

Se debería controlar el acceso a la información y a los procesos del negocio, en base a los requisitos del negocio y de seguridad.

Esto debería tomar en cuenta las políticas para la autorización y diseminación de la información.

9.1.1 Política de control de acceso

9.1.1.1 Política y requisitos del negocio

Se deberían definir y documentar los requisitos del negocio para el control de acceso. Se deberían establecer claramente las reglas y derechos del control de acceso de cada usuario o grupo de usuarios en la declaración de la política de acceso.

Los usuarios y los proveedores de servicios deberían hacer una declaración clara de que cumplen con los requisitos del negocio en los controles de acceso.

La política debería tomar en cuenta lo siguiente:

- a) los requisitos seguridad de las aplicaciones individuales del negocio;
- b) identificación de toda la información relacionada con las aplicaciones del negocio;
- c) políticas para la diseminación y autorización de la información, por ejemplo, la necesidad de conocer los principios y los niveles de seguridad y la clasificación de la información;
- d) consistencia entre el control de acceso y las políticas de clasificación de la información de diferentes sistemas y redes;
- e) legislación pertinente y cualquier obligación contractual relacionada con la protección de acceso a datos o servicios (ver cláusula 12);

NCh2777

- f) perfiles de acceso de usuario normalizado para una categoría de trabajo común;
- g) gestión de los derechos de acceso en un ambiente distribuido y en red que reconoce todos los tipos de conexiones disponibles.

9.1.1.2 Reglas del control de acceso

En la especificación de las reglas de control de acceso, se debería tener cuidado en considerar lo siguiente:

- a) diferenciación entre reglas que siempre se deben exigir y reglas que son opcionales o condicionales;
- b) establecimiento de reglas basadas en la premisa se debe prohibir a menos que expresamente se permita más que en la regla débil todo está generalmente permitido a menos que expresamente se prohíba;
- c) los cambios en las etiquetas de la información (ver 5.2) que se inician automáticamente por los equipos de procesamiento de la información y aquellos que se inician a discreción de un usuario;
- d) los cambios en el permiso de usuarios que se inician automáticamente por el sistema de información y aquellos que se inician por un administrador;
- e) reglas que necesitan aprobación del administrador u otra aprobación antes de la publicación y aquellas que no.

9.2 Gestión de acceso de usuario

Objetivo: Prevenir el acceso no autorizado a los sistemas de información.

Los procedimientos formales deberían estar en el sitio para controlar la asignación de derechos de acceso a los servicios y sistemas de información.

Los procedimientos deberían cubrir todas las etapas en el ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta el registro final de usuarios quienes ya no necesitan acceder a los servicios y sistemas de información. Se debería dar especial atención cuando sea apropiado, a la necesidad de controlar la asignación de derechos de acceso privilegiados, que permiten a los usuarios anular los controles del sistema.

9.2.1 Registro de usuario

Debería existir un procedimiento de registro formal de usuario y de borrado de registro para otorgar el acceso a todos los servicios y sistemas de información multiusuario.

El acceso a servicios de información multiusuario se debería controlar a través de un proceso de registro formal de usuario, el que debería incluir:

- a) usar un único user IDs de modo que los usuarios se puedan conectar y hacer responsables de sus acciones. El uso de IDs de grupo se debería sólo permitir donde ello sea apropiado para realizar algún trabajo;
- b) verificar que el usuario tenga autorización del propio sistema para el uso del sistema de información o servicio. También puede ser apropiada una aprobación separada de la dirección de los derechos de acceso;
- c) verificar que el nivel de acceso que se otorga sea apropiado a los propósitos del negocio (ver 9.1) y que sea consistente con la política de seguridad organizacional, por ejemplo, no comprometer la separación de las obligaciones (ver 8.1.4);
- d) entregar a los usuarios una declaración escrita de sus derechos de acceso;
- e) requerir a los usuarios firmar las declaraciones que indican que ellos entienden las condiciones de acceso;
- f) asegurar que los proveedores de servicio no provean servicio hasta que los procedimientos de autorización estén completos;
- g) mantener un registro formal de todas las personas registradas para el uso del servicio;
- h) retirar inmediatamente los derechos de acceso de usuarios a quienes cambiaron de trabajo o dejaron la organización;
- i) verificación y remoción periódica de user IDs y cuentas redundantes;
- j) asegurar que las user IDs redundantes no se emitan a otros usuarios.

Se debería considerar la inclusión de cláusulas en el contrato del personal y en los contratos de servicios que especifiquen sanciones si el personal o agentes de servicio intenta un acceso no autorizado (ver 6.1.4 y 6.3.5).

9.2.2 Gestión de privilegio

Se debería restringir y controlar la asignación y el uso de privilegios (cualquier característica o facilidad de un sistema de información multiusuario que permita al usuario pasar por sobre el sistema o por sobre los controles de la aplicación). A menudo se encuentra que el uso inapropiado de privilegios del sistema es el factor que más contribuye en las fallas por violación de los sistemas.

Los sistemas multiusuario que requieren protección contra el acceso no autorizado deberían tener la asignación de privilegios controlada mediante un proceso de autorización formal. Se deberían considerar los pasos siguientes:

- a) Los privilegios asociados con cada producto del sistema, por ejemplo, sistema operativo, sistema de gestión de la base de datos y de cada aplicación, se deberían identificar las categorías del personal a las que ellos serán asignados.
- b) Asignar los privilegios a individuos en base a una necesidad de uso y en base a un evento por evento, es decir, la necesidad mínima de sus roles funcionales y sólo cuando se necesite.
- c) Mantener un proceso de autorización y un registro de privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo.
- d) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.
- e) Asignar los privilegios a una identidad de usuario diferente de aquella que se utiliza para el uso normal del negocio.

9.2.3 Gestión de contraseña de usuario

Las contraseñas son una forma común de validar la identidad del usuario para acceder a un sistema de información o servicio. La asignación de contraseña se debería controlar mediante un proceso formal de gestión, un acercamiento a esto debería:

- a) requerir que los usuarios firmen una declaración de mantenimiento confidencial de las contraseñas personales, y de las contraseñas de grupo solamente dentro de los miembros del grupo (esto se podría incluir en los términos y condiciones de empleo, ver 6.1.4);
- b) asegurar, cuando sea necesario que los usuarios mantengan sus propias contraseñas, que ellos estén provistos inicialmente con una contraseña temporal segura y que ellos sean obligados a cambiarla inmediatamente. Las contraseñas temporales que se proveen cuando el usuario olvidó la suya, se deberían proporcionar siguiendo una identificación positiva del usuario;

- c) requerir contraseñas temporales para entregarlas a los usuarios de una manera segura. Se debería evitar el uso de terceras partes o mensajes de correo electrónico no protegido (texto en claro). Los usuarios deberían dar un acuso recibo, de conocimiento de la contraseña.

Las contraseñas nunca se deberían almacenar en un computador en forma desprotegida. También están disponibles otras tecnologías para la identificación de usuario y autenticación, tal como las biométricas, por ejemplo, verificación de huella digital, verificación de firma y uso de tokens, por ejemplo, tarjetas inteligentes, que se deberían considerar si son apropiadas.

9.2.4 Revisión de los derechos de acceso de usuario

Para mantener un control efectivo del acceso a los datos y servicios de información, la dirección debería tener un proceso formal para revisar a intervalos regulares los derechos de acceso de usuario, de modo que:

- a) los derechos de acceso de usuario se revisen a intervalos regulares (se recomienda un período de seis meses) y después de cualquier cambio (ver 9.2.1);
- b) las autorizaciones para derechos de acceso privilegiado (ver 9.2.2) se deberían revisar a intervalos más frecuentes; se recomienda un período de tres meses;
- c) las asignaciones de privilegio se revisen a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados.

9.3 Responsabilidades del usuario

Objetivo: Prevenir el acceso de usuario no autorizado.

La cooperación de los usuarios autorizados es esencial para una efectiva seguridad.

Los usuarios deberían tener conciencia de sus responsabilidades para mantener efectivos los controles de acceso, particularmente con relación al uso de la contraseña y la seguridad de los equipos en uso.

9.3.1 Uso de la contraseña

Los usuarios deberían tener una buena práctica de seguridad en la selección y uso de las contraseñas.

El proveer de contraseña es una forma de validar la identidad del usuario y así establecer los derechos de acceso a las instalaciones de procesamiento de la información o servicios. Todos los usuarios deberían estar notificados de:

- a) mantener en forma confidencial las contraseñas;
- b) evitar mantener un registro de contraseñas en papel, a menos que éste se pueda guardar en forma segura;

NCh2777

- c) cambiar las contraseñas cuando quiera que exista una indicación de un posible compromiso de la contraseña o del sistema;
- d) seleccionar la calidad de la contraseña con una longitud mínima de seis caracteres los que:
 - d.1) sean fácil de recordar;
 - d.2) no estén basados en cualquier cosa o en alguna persona que se podría suponer fácilmente u obtener usando la información relacionada con la persona, por ejemplo, nombres, números telefónicos y fechas de nacimientos, etc.;
 - d.3) estén libre de caracteres idénticos consecutivos o grupos todos numéricos o todos alfabéticos.
- e) cambiar las contraseñas a intervalos regulares o basado en el número de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar más frecuentemente que las contraseñas normales) y evitar el reuso o reciclaje de contraseñas viejas;
- f) cambiar la contraseña temporal al abrir la primera sesión;
- g) no incluir la contraseña en cualquier proceso de abrir sesión automatizado, por ejemplo, almacenada en una macro o en una función clave;
- h) no compartir las contraseñas de usuarios individuales.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y es necesario que mantengan múltiples contraseñas, ellos deberían ser notificados que pueden usar una única contraseña de calidad [ver d) anterior] en todos los servicios que proveen un nivel razonable de protección para la contraseña almacenada.

9.3.2 Equipos desatendidos

Los usuarios se deberían asegurar que los equipos desatendidos tengan una protección apropiada. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivo, pueden necesitar una protección específica a los accesos no autorizados cuando se dejan desatendidos por un período largo de tiempo. Todos los usuarios y personal externo deberían tener conocimiento de los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos, como también sus responsabilidades para implementar tal protección. Los usuarios deberían ser notificados para:

- a) cerrar las sesiones activas en el computador cuando finaliza la labor, a menos que éstas se puedan asegurar mediante un apropiado mecanismo de traba, por ejemplo, con protector de pantalla con una contraseña protegida;

- b) cerrar las sesiones de los computadores principales cuando la sesión finaliza (es decir, no precisamente apagar el terminal o PC);
- c) asegurar los terminales o PC del uso no autorizado, mediante una clave de traba o un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

9.4 Control de acceso a la red

Objetivo: Protección de los servicios de red.

Se debería controlar el acceso a los servicios de red externo e internos.

Esto es necesario para asegurar que los usuarios quienes tienen acceso a redes y servicios de red no comprometan la seguridad de estos servicios mediante el aseguramiento de:

- a) interfaces apropiadas entre la red de la organización y redes de otras organizaciones o redes públicas;
- b) mecanismos de autenticación apropiados para usuarios y equipos;
- c) control del acceso de usuario a los servicios de información.

9.4.1 Política de uso de los servicios de red

Las conexiones inseguras a los servicios de red pueden afectar a toda la organización. Los usuarios deberían tener acceso directo a los servicios que ellos han sido específicamente autorizados para usar. Este control es particularmente importante para aplicaciones críticas o sensibles del negocio, conectadas a la red o para usuarios en ubicaciones de alto riesgo, por ejemplo, en áreas públicas o externas que están fuera del control y de la gestión de seguridad de la organización.

Se debería formular una política relativa al uso de redes y servicios de red. Esto debería cubrir:

- a) las redes y servicios de red a las que el acceso está permitido;
- b) procedimientos de autorización para determinar quien tiene permitido acceder a qué redes y servicios de red;
- c) controles de gestión y procedimientos para proteger el acceso a las conexiones de la red y servicios de red.

Esta política debería ser consistente con la política de control de acceso del negocio (ver 9.1).

9.4.2 Ruta forzada

Puede ser necesario controlar la ruta desde el terminal de usuario al servicio computacional. Las redes se diseñan para permitir compartir el máximo de los recursos y flexibilidad de rutas. Estas características también pueden proveer oportunidades para un acceso no autorizado a las aplicaciones del negocio o uso no autorizado de las instalaciones de información. Incorporar controles que restrinjan la ruta entre un terminal de usuario y los servicios computacionales de modo que el usuario para acceder sea autorizado, por ejemplo, se pueden reducir tales riesgos creando una ruta forzada.

El objetivo de una ruta forzada es prevenir que algunos usuarios seleccionen rutas externas a la ruta entre el terminal de usuario y los servicios que el usuario está autorizado a acceder.

Esto generalmente necesita la implementación de una variedad de controles en diferentes puntos de la ruta. El principio es limitar las opciones de rutas en cada punto de la red, mediante la elección predefinida.

Ejemplos de esto son los que siguen:

- a) asignando líneas dedicadas o números telefónicos;
- b) puertas de conexión automática a las aplicaciones específicas del sistema o gateways de seguridad;
- c) menú limitado u opciones de submenú para usuarios individuales;
- d) impidiendo la transferencia a redes no limitadas;
- e) imponiendo el uso de una aplicación específica del sistema y/o gateways de seguridad para los usuarios de redes externas;
- f) controlando activamente la fuente permitida para enviar comunicaciones, vía gateways de seguridad, por ejemplo, con firewalls;
- g) restringiendo el acceso a la red, configurando un dominio lógico separado, por ejemplo redes privadas virtuales, para grupos de usuarios dentro de la organización (ver también 9.4.6).

Los requisitos para una ruta forzada, se deberían basar en la política de control de acceso del negocio (ver 9.1).

9.4.3 Autenticación del usuario para conexiones externas

Las conexiones externas proveen un acceso potencial no autorizado a la información del negocio, por ejemplo, el acceso por métodos de discado. Por lo tanto, el acceso de usuarios remotos debería estar sujeto a autenticación. Hay diferentes tipos de métodos de autenticación, algunos de estos proveen mayor nivel de protección que otros, por ejemplo, métodos basados en el uso de técnicas criptográficas que proveen autenticación fuerte. De la evaluación del riesgo, es importante determinar el nivel de protección requerido. Esto se necesita para la selección apropiada de un método de autenticación.

La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica en base a la criptografía, tokens, o un protocolo desafío/respuesta. También se pueden usar las líneas privadas dedicadas o una instalación que verifique la dirección del usuario de red para proveer seguridad del origen de la conexión.

Los controles y procedimientos del discado de retorno, por ejemplo el uso de modems de discado de retorno, pueden proveer protección contra las conexiones no autorizadas y no deseadas a las instalaciones de procesamiento de información de una organización. Este tipo de control autentica a los usuarios que tratan de establecer una conexión a una red de una organización desde ubicaciones remotas. Cuando se usa este control, una organización no debería usar los servicios de red que incluyen desvío de llamadas o si ellos se usan, se debería deshabilitar el uso de tal característica para evitar deficiencias asociadas con el desvío de llamadas. También es importante que el proceso de llamada de retorno incluya el aseguramiento que realmente ocurre la desconexión en el lado de la organización. De otra manera, el usuario remoto podría mantener la línea abierta tratando que ocurra la verificación de llamada de retorno. Los controles y procedimientos de llamada de retorno se deberían probar a fondo para evitar esta posibilidad.

9.4.4 Autenticación de nodo

Una instalación para una conexión automática a un computador remoto podría proveer un modo de obtener acceso no autorizado a la aplicación del negocio. Por lo tanto se deberían autenticar las conexiones a sistemas computacionales remotos. Esto es especialmente importante si la conexión usa una red que es externa al control de la gestión de seguridad de la organización. En 9.4.3 se indican algunos ejemplos de autenticación y cómo se puede lograr.

La autenticación de nodo puede servir como un modo alternativo de autenticación de grupos de usuarios remotos cuando ellos se conectan a una instalación computacional compartida y segura (ver 9.4.3).

9.4.5 Protección de puerta diagnóstico remoto

El acceso a las puertas de diagnóstico se controlan en forma segura. Diversos computadores y sistemas de comunicación se instalan con equipos de diagnóstico de discado remoto para el uso de los ingenieros de mantenimiento. Estas puertas de diagnóstico proveen una forma de acceso no autorizado, si están desprotegidas. Por lo tanto ellas se deberían proteger con un mecanismo de seguridad apropiado, por ejemplo, un acceso con clave y un procedimiento para asegurar que ellas son accesibles sólo por acuerdo entre el directivo del servicio computacional y el personal de apoyo del hardware/software que requiere acceso.

9.4.6 Separación en las redes

Las redes están aumentando su extensión más allá de los límites tradicionales de la organización, como los socios del negocio que están configurados para requerir interconexión o compartir las instalaciones de red y de procesamiento de la información. Tales extensiones pueden aumentar el riesgo de acceso no autorizado a los sistemas de información existentes que usan la red, algunos de los cuales podría necesitar protección de otros usuarios de red debido a su sensibilidad o criticidad. En tales circunstancias, se debería considerar la introducción de controles dentro de la red, para separar grupos de servicios de información, usuarios y sistemas de información.

Un método para controlar la seguridad de las redes grandes es dividir las redes lógicas separadas, por ejemplo, un dominio de la red interna de la organización y un dominio de la red externa, cada uno protegido mediante un perímetro de seguridad definido. Tal perímetro se puede implementar por la instalación de un gateway de seguridad entre las dos redes que se interconectan, para el control de acceso y del flujo de información entre los dos dominios (ver 9.4.7 y 9.4.8) y bloquear el acceso no autorizado, de acuerdo con la política de control de acceso de la organización (ver 9.1). Un ejemplo de este tipo de gateway es el que comúnmente se conoce como firewall.

El criterio para la separación de redes en dominios se debería basar en la política de control de acceso y los requisitos de acceso (ver 9.1), y tomar en cuenta también el costo relativo y el comportamiento del impacto de incorporar una ruta apropiada de una red o de la tecnología de un gateway (ver 9.4.7 y 9.4.8).

9.4.7 Control de conexión de red

Los requisitos de la política de control de acceso para las redes compartidas, especialmente aquellas que extienden los límites de la organización, pueden requerir la incorporación de controles para restringir la capacidad de conexión de los usuarios. Tales controles se pueden implementar en los gateways de la red que filtran el tráfico por medio de reglas o tablas pre definidas. Las restricciones aplicadas se deberían basar en la política de acceso y en los requisitos de las aplicaciones del negocio (ver 9.1), y se deberían mantener y actualizar como corresponde.

Ejemplos de aplicaciones a las que se deberían aplicar restricciones son:

- a) correo electrónico;
- b) transferencia de archivos en un sentido;
- c) transferencia de archivos en ambos sentidos;
- d) acceso interactivo;
- e) enlace de acceso a la red en una hora del día o fecha.

9.4.8 Control de enrutamiento de red

Las redes compartidas, especialmente aquellas que extienden los límites de la organización, pueden necesitar la incorporación de controles de enrutamiento para asegurar que las conexiones al computador y el flujo de información no violan la política de control de acceso de las aplicaciones del negocio (ver 9.1). Este control a menudo es esencial para las redes compartidas con usuarios de terceras partes (no organizaciones).

Los controles de enrutamiento se deberían basar en un origen seguro y en mecanismos de verificación de las direcciones de destino. La traducción de direcciones de red también es un mecanismo muy útil para aislar las redes y prevenir rutas que se propaguen de la red de una organización a la red de otra. Ello se puede implementar por software o hardware. Personal de implementación debería tener conocimiento de la fortaleza de cualquier mecanismo desplegado.

9.4.9 Seguridad de los servicios de red

Está disponible una amplia variedad de servicios de redes privadas o públicas, algunas de las cuales ofrecen servicios de valor agregado. Los servicios de redes pueden tener características de seguridad complejas o únicas. Las organizaciones que usan servicios de redes se deberían asegurar que se provea una clara descripción de las características de la seguridad de todos los servicios.

9.5 Control de acceso a la operación del sistema

Objetivo: Evitar el acceso no autorizado a computadores.

Las instalaciones de seguridad al nivel de operación del sistema deberían restringir el acceso a los recursos computacionales. Estas instalaciones deberían ser capaces de lo siguiente:

- a) identificar y verificar la identidad y si es necesario el terminal o la ubicación de cada usuario autorizado;
- b) registrar los accesos exitosos y fallidos al sistema;
- c) proveer formas apropiadas de autenticación; si se usa un sistema de gestión de contraseña, se debería asegurar la calidad de la contraseña [ver 9.3.1 d)];
- d) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

Otros métodos de control de acceso, tales como desafío/respuesta, están disponibles si se justifican en base al riesgo del negocio.

9.5.1 Identificación automática del terminal

Se debería considerar la identificación automática del terminal para autenticar las conexiones de ubicaciones específicas y de equipos portátiles. La identificación automática del terminal es una técnica que se puede usar cuando es importante que la sesión se pueda iniciar solamente desde una ubicación o un terminal de computador particular. Se puede usar un identificador incluido o adjunto al terminal para indicar que este terminal particular tiene permitido iniciar o recibir transacciones específicas. Puede ser necesario aplicar protección física al terminal, para mantener la seguridad del identificador del terminal. Una variedad de otras técnicas también se pueden usar para autenticar los usuarios (ver 9.4.3).

9.5.2 Procedimientos para abrir una sesión en el terminal

El acceso a los servicios de información se debería alcanzar vía un proceso para abrir sesión seguro. El procedimiento para abrir una sesión en el sistema computacional se debería diseñar para minimizar la oportunidad de acceso no autorizado. Por lo tanto el procedimiento par abrir una sesión debería divulgar el mínimo de información relativa al sistema, con el fin de evitar proveer la asistencia innecesaria a un usuario no autorizado. Un buen procedimiento para abrir una sesión debería:

- a) no mostrar los identificadores del sistema o aplicación hasta que el proceso de abrir una sesión se haya completado exitosamente;
- b) mostrar un aviso de advertencia general, que indique que el computador sólo se debería acceder por usuarios autorizados;

- c) no proveer mensajes de ayuda durante el procedimiento de registro que ayudarían a un usuario no autorizado;
- d) validar la información para abrir una sesión sólo al final de todos los datos de entrada. Si aparece una condición de error, el sistema no debería indicar que parte de los datos son correctos o incorrectos;
- e) limitar el número de intentos no exitosos permitidos, para abrir una sesión (se recomienda tres) y considerar:
 - e.1) registrar los intentos no exitosos;
 - e.2) forzar un tiempo de retardo antes que los nuevos intentos de abrir una sesión se permitan o se rechace cualquier nuevo intento sin autorización específica;
 - e.3) desconectar los enlaces de datos;
- f) limitar el máximo y mínimo tiempo permitido para el procedimiento de abrir una sesión. Si se excede, el sistema debería terminar el procedimiento de abrir una sesión;
- g) mostrar la información siguiente al terminar la última sesión exitosa:
 - g.1) fecha y hora de la sesión exitosa anterior;
 - g.2) detalles de cualquier intento de sesión no exitosa, desde la última sesión exitosa.

9.5.3 Identificación de usuario y autenticación

Todos los usuarios (incluyendo el personal de apoyo técnico, tales como operadores, administradores de red, programadores del sistema y administradores de base de datos) deberían tener un identificador único (user ID) para su uso exclusivo y personal, de modo que las actividades se puedan seguir posteriormente debido a la responsabilidad individual. Las user IDs no deberían dar ninguna indicación de los niveles de privilegios de usuarios (ver 9.2.2), por ejemplo, directivo, supervisor.

En circunstancias excepcionales, donde exista un claro beneficio del negocio, se puede usar una user ID en un trabajo específico o compartida con un grupo de usuarios. Para tales casos se debería documentar la aprobación de la dirección. Se pueden necesitar controles adicionales para mantener la responsabilidad.

Hay varios procedimientos de autenticación, que se pueden usar para comprobar la identidad exigida de un usuario. Las contraseñas (ver también 9.3.1 y más abajo) son una manera muy común de proveer identificación y autenticación (I&A) en base a un secreto que sólo el usuario conoce. Lo mismo también se logra con técnicas criptográficas y protocolos de autenticación.

Los objetos tales como, tokens de memoria o tarjetas inteligentes que poseen los usuarios también se pueden usar para I&A. Tecnologías de autenticación biométrica que usan características únicas o atributos de un individuo también se pueden usar para autenticar la identidad de la persona. Una combinación de tecnologías y mecanismos de enlace seguro llevan a una autenticación más fuerte.

9.5.4 Sistema de gestión de contraseña

Las contraseñas son una de las principales formas de validar la autorización de un usuario para acceder a un servicio computacional. Los sistemas de gestión de contraseña deberían proveer una instalación efectiva e interactiva, que asegure la calidad de las contraseñas (ver 9.3.1 para una guía de uso de contraseñas).

Algunas aplicaciones requieren contraseñas de usuario que son asignadas por una autoridad independiente. En la mayoría de los casos las contraseñas se seleccionan y mantienen por los usuarios.

Un buen sistema de gestión de contraseñas debería:

- a) imponer el uso de contraseñas individuales para mantener la responsabilidad personal;
- b) cuando sea apropiado, permitir a los usuarios seleccionar y cambiar su propia contraseña e incluir un procedimiento de confirmación para permitir errores de entrada;
- c) imponer una elección de contraseña de calidad como se describe en 9.3.1;
- d) cuando los usuarios mantienen sus propias contraseñas, imponer cambios de contraseña como se describe en 9.3.1;
- e) cuando los usuarios seleccionan las contraseñas, obligarlos a cambiar la contraseña temporal al abrir la primera sesión (ver 9.2.3);
- f) mantener un registro de contraseñas anteriores de usuarios, por ejemplo, de los 12 meses anteriores y evitar su uso;
- g) no mostrar la contraseña en la pantalla cuando se está ingresando;
- h) almacenar los archivos de contraseña separadamente de los datos de la aplicación del sistema;
- i) almacenar las contraseñas en forma encriptada usando un algoritmo de encriptación de un sentido;
- j) cambiar la contraseña pre establecida por el proveedor, inmediatamente después de la instalación del software.

9.5.5 Uso de los utilitarios del sistema

La mayoría de las instalaciones computacionales tienen uno o más programas utilitarios que pueden ser capaces de anular los controles de la aplicación y del sistema. Es esencial que se restrinja y se controle su uso rigurosamente. Se deberían considerar los controles siguientes:

- a) uso de procedimientos de autenticación para los utilitarios del sistema;
- b) separación de los utilitarios del sistema, de los software de aplicación;
- c) limitación del uso de los utilitarios del sistema al mínimo número práctico de usuarios de confianza autorizados;
- d) autorización para el uso ad hoc de utilitarios del sistema;
- e) limitación de la disponibilidad de los utilitarios del sistema, por ejemplo, por la duración de un cambio autorizado;
- f) registro de todos los usos de los utilitarios del sistema;
- g) definición y documentación de los niveles de autorización para los utilitarios del sistema;
- h) remoción de todo el software de apoyo innecesario al software y utilitarios del sistema.

9.5.6 Alarma de coacción para salvaguardar los usuarios

La provisión de una alarma de coacción se debería considerar para usuarios quienes pueden ser objeto de coacción. La decisión de suministrar tal alarma se debería basar en la evaluación de los riesgos. Deberían existir los procedimientos y responsabilidades para responder a la alarma de coacción.

9.5.7 Time out del terminal

Los terminales inactivos en ubicaciones de alto riesgo, por ejemplo, en áreas externas o públicas, fuera de la gestión de seguridad de la organización, o sistemas de servidor de alto riesgo, se deberían apagar después de un período definido de inactividad para evitar el acceso de personas no autorizadas. Esta facilidad de time out debería limpiar la pantalla del terminal y cerrar la aplicación y las sesiones de red después de un período definido de inactividad. El retardo de time out debería reflejar los riesgos de seguridad del área y los usuarios del terminal.

Se puede proveer una forma limitada de la facilidad de time out para algunos computadores personales, esto es limpiar la pantalla y prevenir el acceso no autorizado pero no cerrar la aplicación o la sesión de red.

9.5.8 Limitación del tiempo de conexión

Las restricciones en los tiempos de conexión se deberían proveer adicionalmente a la seguridad de las aplicaciones de alto riesgo. Limitando el período de conexión del terminal se permite a los servicios computacionales reducir la ventana de oportunidad de acceso no autorizado. Tal control debería considerar las aplicaciones computacionales sensibles, especialmente aquellas con terminales instalados en ubicaciones de alto riesgo, por ejemplo, en áreas públicas o externas que están fuera de la gestión de seguridad de la organización. Ejemplos de tales restricciones incluyen:

- a) usar intervalos de tiempo predeterminados, por ejemplo, transmisión de archivos batch, o sesiones interactivas regulares de corta duración;
- b) restringir los tiempos de conexión a horas de oficina si no existe necesidad de sobretiempo o de operación en horas extendidas.

9.6 Control de acceso a la aplicación

Objetivo: Prevenir el acceso no autorizado a la información que se mantiene en los sistemas de información. Se deberían usar instalaciones de seguridad para restringir el acceso dentro de las aplicaciones del sistema.

El acceso lógico al software y a la información se debería restringir a usuarios autorizados. Las aplicaciones deberían:

- a) controlar el acceso de los usuarios a la información y a las funciones de la aplicación del sistema, conforme con una política definida de control de acceso del negocio;
- b) proveer protección contra el acceso no autorizado a cualquier utilitario y software del sistema operativo que sea capaz de pasar por sobre el sistema o los controles de la aplicación;
- c) no comprometer la seguridad de otros sistemas con los que se comparte los recursos de información;
- d) ser capaz de proveer acceso a la información solamente al dueño, a otros individuos designados y autorizados o a grupos definidos de usuarios.

9.6.1 Restricción de acceso a la información

Los usuarios de las aplicaciones del sistema, incluidos el personal de apoyo, deberían tener acceso a la información y a las funciones de la aplicación del sistema de acuerdo a la política de control de acceso, en base a los requisitos de la aplicación individual del negocio y consistente con la política de acceso a la información de la organización (ver 9.1). Se debería considerar la aplicación de los controles siguientes con el fin de apoyar los requisitos de restricción de acceso:

- a) proveer menús para controlar el acceso a las funciones de la aplicación;

- b) restringir a los usuarios el conocimiento de la información o de las funciones de aplicación del sistema a las cuales ellos no están autorizados a acceder, con una edición apropiada de la documentación de usuario;
- c) controlar los derechos de acceso de usuarios, por ejemplo, leer, escribir, borrar o ejecutar;
- d) asegurar que las salidas de información sensible que manipulan las aplicaciones del sistema contengan sólo la información que es pertinente al uso de la salida y que se envíen sólo a los terminales y ubicaciones autorizadas, incluyendo la revisión periódica de tales salidas para asegurar que se retire la información redundante.

9.6.2 Aislamiento del sistema sensible

Los sistemas sensibles pueden necesitar un ambiente computacional dedicado (aislado). Algunas aplicaciones del sistema son suficientemente sensibles a pérdidas potenciales de modo que ellas requieren manipulación especial. La sensibilidad puede indicar que la aplicación del sistema se debería ejecutar en un computador dedicado, debería solamente compartir recursos con las aplicaciones confiables, o no tener limitaciones. Aplicar las consideraciones siguientes:

- a) La sensibilidad de una aplicación del sistema se debería identificar explícitamente y documentar por el dueño de la aplicación (ver 4.1.3).
- b) Cuando una aplicación sensible se ejecuta en un ambiente compartido, se deberían identificar las aplicaciones de los sistemas con los cuales compartirá recursos y debería estar de acuerdo con el dueño de la aplicación sensible.

9.7 Monitoreo de uso y acceso al sistema

Objetivo: Detectar actividades no autorizadas.

Los sistemas se deberían monitorear para detectar desviación de la política de control de acceso y registrar los eventos que se pueden monitorear para proveer evidencias en el caso de incidentes de seguridad.

El sistema de monitoreo permite, revisar la efectividad de los controles adoptados y verificar la conformidad con el modelo de la política de acceso (ver 9.1).

NCh2777

9.7.1 Registro de evento

Se deberían auditar los registros de excepciones y otros eventos de seguridad pertinentes y guardarlos por un período acordado, para ayudar en futuras investigaciones y monitoreo del control de acceso.

La auditoría de los registros también debería incluir:

- a) user IDs;
- b) fechas y horas de abrir y cerrar sesiones;
- c) identificación del terminal o ubicación si es posible;
- d) registros de intentos de acceso al sistema exitosos y rechazados;
- e) registros de intentos de acceso a los datos y a otros recursos, exitosos y rechazados.

Puede ser necesario que ciertas auditorías se archiven como parte de la política de conservación de registros o debido a los requisitos de reunir evidencias (ver también cláusula 12).

9.7.2 Monitoreo del uso del sistema

9.7.2.1 Procedimientos y áreas de riesgos

Se deberían establecer procedimientos de monitoreo del uso de las instalaciones de procesamiento de la información. Tales procedimientos son necesarios para asegurar que los usuarios realicen solamente actividades que se hayan autorizado explícitamente. El nivel de monitoreo necesario para las instalaciones individuales se debería determinar por una evaluación del riesgo. Las áreas que se deberían incluir:

- a) acceso autorizado, que incluye detalles como:
 - a.1) el user ID;
 - a.2) la fecha y hora de los eventos claves;
 - a.3) el tipo de eventos;
 - a.4) los archivos accedidos;
 - a.5) los programas/ utilitarios que se usan.

- b) todas las operaciones privilegiadas, tales como:
 - b.1) uso de cuenta de supervisor;
 - b.2) partida y detención del sistema;
 - b.3) conexión/ desconexión de dispositivos E/S.
- c) intentos de acceso no autorizados, tales como:
 - c.1) intentos fallidos;
 - c.2) violaciones a las políticas de acceso y avisos de gateways y firewalls;
 - c.3) alertas de los sistemas propietarios de detección de intrusión.
- d) sistemas de alertas o de fallas, tal como:
 - d.1) alerta o mensajes de consola;
 - d.2) registros de excepciones del sistema;
 - d.3) alarmas de gestión de red.

9.7.2.2 Factores de riesgo

El resultado de las actividades de monitoreo se debería revisar regularmente. La frecuencia de las revisiones debería depender de los riesgos involucrados. Los factores de riesgo que se deberían considerar incluyen:

- a) la criticidad de los procesos de la aplicación;
- b) el valor, sensibilidad o criticidad de la información involucrada;
- c) la experiencia pasada de la infiltración y mal uso del sistema;
- d) la extensión de la interconexión del sistema (particularmente en redes públicas).

9.7.2.3 Registro y revisión de eventos

Una revisión de los eventos involucra la comprensión de las amenazas enfrentadas por el sistema y la manera en que éstas pueden aparecer. Ejemplos de eventos que pueden necesitar investigación más amplia es el caso de los incidentes de seguridad indicados en 9.7.1.

Los registros del sistema a menudo contienen un gran volumen de información, mucho de éste es ajeno al monitoreo de seguridad. Para ayudar a identificar los eventos significativos con propósitos de monitoreo de seguridad, se debería considerar copiar los mensajes tipos apropiados automáticamente a un segundo registro, y/o el uso de los utilitarios adecuados del sistema o las herramientas de auditoría para analizar archivos.

Cuando se asigna la responsabilidad de revisar el registro, se debería considerar una separación de los roles entre la(s) persona(s) que efectúa(n) la revisión y aquella cuyas actividades están siendo monitoreadas.

Particular atención se debería dar a la seguridad de las instalaciones de registros debido a que si se altera puede proveer una falsa sensación de seguridad. Los controles deberían ayudar a proteger de los cambios no autorizados y de los problemas operacionales, incluyendo:

- a) el registro que está siendo desactivado;
- b) las alteraciones de los tipos de mensajes que son registrados;
- c) el archivo de registro que está siendo editado o borrado;
- d) el dispositivo de archivo de registro que esté lleno y, si está defectuoso para registrar eventos o para la sobre escritura.

9.7.3 Sincronización del reloj

Es importante el ajuste correcto del reloj del computador para resguardar la seguridad de registros de auditoría, los que puedan ser necesarios para las investigaciones o como evidencia en casos legales o disciplinarios. Los registros de auditoría inexactos pueden obstruir tales investigaciones y dañar la credibilidad de tal evidencia.

Cuando un computador o dispositivo de comunicación tiene la capacidad de operar un reloj en tiempo real, debería ajustarse a un estándar acordado, por ejemplo, la hora coordinada universal (UCT) u hora estándar local. Como se sabe que algunos relojes tienen desfase con el tiempo, debería existir un procedimiento que verifique y corrija cualquier variación significativa.

9.8 Computadores móviles y teletrabajo

Objetivo: Resguardar la seguridad de la información cuando se usen computadores móviles y equipos de teletrabajo.

La protección necesaria debería estar en proporción con los riesgos que causa esta manera específica de trabajo. Cuando se usan computadores móviles se deberían considerar los riesgos de trabajar en un ambiente no protegido y aplicar la protección apropiada. En el caso de teletrabajo la organización debería aplicar protección al sitio de teletrabajo y asegurar que para esta forma de trabajo la configuración adecuada está instalada.

9.8.1 Computadores móviles

Cuando se usen equipos de computadores móviles, por ejemplo, notebooks, palmtops, laptops y teléfonos móviles, se debería tener especial cuidado para asegurar que la información del negocio no se comprometa. Se debería adoptar una política formal que tome en cuenta los riesgos de trabajar con equipos de computadores móviles, en particular en ambientes no protegidos. Por ejemplo, tal política debería incluir los requisitos de protección física, controles de acceso, técnicas de criptografía, respaldos y protección antivirus. Esta política también debería incluir reglas y consejos en la conexión de equipos móviles a redes y una guía para el uso de estos equipos en los lugares públicos.

Se debería tener cuidado cuando se usen equipos de computadores móviles en lugares públicos, salas de reunión y otras áreas no protegidas externas a las instalaciones de la organización. Se debería tener protección en el sitio para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos equipos, por ejemplo, el uso de técnicas de criptografía (ver 10.3).

Es importante cuando tales equipos se usen en lugares públicos tener cuidado para evitar el riesgo de que lo observen y los usen personas no autorizadas. Los procedimientos contra el software malicioso deberían estar disponibles y mantenerlos actualizados (ver 8.3). Deberían estar disponibles equipos para permitir un rápido y fácil respaldo de la información. Estos respaldos deberían dar una protección adecuada, por ejemplo, contra robos y pérdida de información.

Una protección apropiada se debería dar a los equipos móviles conectados a las redes. El acceso remoto a la información del negocio vía una red pública usando un equipo computador móvil debería suceder solamente después de la identificación y autenticación exitosa y tener los mecanismos de control de acceso apropiado instalados (ver 9.4).

Los equipos de computadores móviles también deberían estar físicamente protegidos contra los robos, especialmente cuando se dejan, por ejemplo, en autos y otros medios de transporte, habitaciones de hoteles, centros de conferencias y lugares de reuniones. Los equipos que contienen información importante del negocio, sensible y/o crítica no se debería dejar desatendido y, cuando sea posible, debería estar físicamente con llave o se deberían usar trabas especiales para asegurarlo. En 7.2.5 se puede encontrar más información respecto a la protección física de los equipos móviles.

Se debería disponer de entrenamiento para el personal que usa computadores móviles, para elevar su conocimiento de los riesgos adicionales que aparecen al trabajar de esta forma y de los controles que se deberían implementar.

9.8.2 Teletrabajo

El teletrabajo usa la tecnología de las comunicaciones para permitir que el personal trabaje remotamente desde un lugar fijo fuera de la ubicación de su organización. La protección adecuada del sitio de teletrabajo debería estar instalada en contra de, por ejemplo, el robo de los equipos y de la información, divulgación no autorizada de la información, acceso remoto no autorizado a los sistemas internos de la organización o mal uso de los equipos. Es importante que el teletrabajo sea autorizado y controlado por la dirección, y que, para esta forma de trabajo las configuraciones adecuadas estén instaladas.

Las organizaciones deberían considerar el desarrollo de una política, procedimientos y normas para el control de las actividades de teletrabajo. Las organizaciones deberían autorizar sólo las actividades de teletrabajo si ellas satisfacen las disposiciones de seguridad apropiadas, existen los controles y cumplen con la política de seguridad de la organización. Se debería considerar lo siguiente:

- a) la existencia de la seguridad física del sitio de teletrabajo, tomando en cuenta la seguridad física del edificio y su ambiente;
- b) el ambiente de teletrabajo propuesto;
- c) los requisitos de seguridad de las comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información que será accesible, el paso por el enlace de comunicación y la sensibilidad del sistema interno;
- d) la amenaza de acceso no autorizado a la información o recursos, de otras personas que usan las acomodaciones del sitio, por ejemplo, la familia y los amigos.

Se debería considerar incluir los controles y disposiciones para:

- a) el suministro de los equipos adecuados y accesorios de almacenamiento para las actividades de teletrabajo;
- b) una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede guardar y los sistemas internos y servicios que el teletrabajador está autorizado a acceder;
- c) el suministro de los equipos de comunicaciones apropiados, incluyendo los métodos para el acceso remoto seguro;
- d) la seguridad física;
- e) reglas y guías en la familia y el acceso de visitas a los equipos e información;
- f) el suministro de apoyo al software y hardware y mantenimiento;
- g) los procedimientos de respaldo y continuidad del negocio;
- h) auditoría y monitoreo de la seguridad;
- i) revocación de la autoridad, derechos de acceso y el retorno de los equipos cuando finalizan las actividades de teletrabajo.

10 Desarrollo y mantenimiento de sistemas

10.1 Requisitos de seguridad de los sistemas

Objetivo: Resguardar que la seguridad esté incorporada en los sistemas de información.

Esto incluye la infraestructura, las aplicaciones del negocio y las aplicaciones desarrolladas por el usuario. El diseño e implementación del proceso del negocio que apoya a la aplicación o servicio puede ser crucial para la seguridad. Los requisitos de seguridad se deberían identificar y acordar antes de desarrollar los sistemas de información.

Todos los requisitos de seguridad, incluyendo la necesidad de las configuraciones de recuperación, se deberían identificar en la fase de requisitos del proyecto, justificándolos, acordándolos y documentándolos, como parte del plan global del negocio, para un sistema de información.

10.1.1 Análisis y especificaciones de los requisitos de seguridad

Las declaraciones de los requisitos para los nuevos sistemas, o para reforzar los sistemas existentes deberían especificar los requisitos de los controles. Tales especificaciones deberían considerar los controles automatizados para incorporarlos al sistema y la necesidad de apoyo de controles manuales. Se deberían aplicar consideraciones similares cuando se evalúan paquetes de software para las aplicaciones del negocio. Si se considera apropiado, la dirección puede hacer uso de productos evaluados y certificados independientemente.

Los requisitos de seguridad y control deberían reflejar el valor de los bienes de información del negocio involucrados y el potencial daño al negocio, que podría resultar de una falla o ausencia de seguridad. El marco para analizar los requisitos de seguridad e identificar los controles para cumplir con ellos es la evaluación y la gestión del 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 de las aplicaciones de los sistemas

Objetivo: Prevenir la pérdida, modificación o mal uso de los datos de usuario en las aplicaciones de los sistemas.

Los controles apropiados y los seguimientos de auditorías o los registros de actividad se deberían diseñar en la aplicación de los sistemas, incluyendo las aplicaciones escritas por el usuario. Estos deberían incluir la validación de los datos de entrada, procesamiento interno y datos de salida.

Se pueden necesitar controles adicionales para los sistemas que procesan bienes críticos de la organización o de valor sensible o tienen un impacto en ella. Tales controles se deberían determinar en base a los requisitos de seguridad y evaluación del riesgo.

10.2.1 Validación de los datos de entrada

Los datos de entrada a las aplicaciones de los sistemas se deberían validar para asegurar que son correctos y apropiados. Se debería aplicar a la entrada una verificación de las transacciones del negocio, datos permanentes (nombres y direcciones, límites de crédito, números de referencia del cliente) y tablas de parámetros (precios de ventas, tasas de conversión de monedas, tasas de impuestos). Se deberían considerar los controles siguientes:

a) entrada dual u otra verificación de la entrada para detectar los errores siguientes:

- a.1) valores fuera de rango;
- a.2) caracteres inválidos en los campos de datos;

- a.3) datos incompletos o equivocados;
- a.4) volumen de datos que exceden los límites inferior y superior;
- a.5) control de los datos inconsistentes o no autorizados.
- b) revisión periódica del contenido de los campos claves o archivos de datos para confirmar su validez e integridad;
- c) inspeccionar los documentos de entrada en papel para verificar cualquier cambio no autorizado en los datos de entrada (todos los cambios a los documentos de entrada se deberían autorizar);
- d) procedimientos para responder a los errores de validación;
- e) procedimientos para probar la credibilidad de los datos de entrada;
- f) definir las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

10.2.2 Control del procesamiento interno

10.2.2.1 Areas de riesgo

Los datos que se han ingresado correctamente se pueden corromper por errores de procesamiento o por actos deliberados. Se debería incorporar en los sistemas la prueba de validación para detectar tal corrupción. El diseño de las aplicaciones debería asegurar que las restricciones se implementan para minimizar el riesgo de fallas de procesamiento que lleven a la pérdida de integridad. Considerar en las áreas específicas la incorporación de:

- a) el uso y ubicación en los programas de las funciones de adición y borrado para implementar cambios a los datos;
- b) los procedimientos para evitar que se ejecuten programas en orden equivocado o que se ejecuten después de una falla en el procesamiento previo (ver también 8.1.1);
- c) el uso de programas correctos para recuperar fallas y asegurar el correcto procesamiento de los datos.

10.2.2.2 Verificaciones y controles

Los controles necesarios dependerán de la naturaleza de la aplicación y del impacto al negocio de cualquier corrupción de los datos. Los ejemplos de verificación que se pueden incorporar incluyen lo siguiente:

- a) controles de sesión o de procesos batch, para conciliar los balances de archivos de datos después de las transacciones de actualización;

- b) controles de balance para verificar la apertura de balances cerrados previamente, a saber:
 - b.1) controles entre ejecuciones;
 - b.2) totales de actualización de archivos;
 - b.3) controles programa a programa;
- c) validación de los datos generados por el sistema (ver 10.2.1);
- d) verificaciones de la integridad de los datos o del software descargado o cargado entre el computador remoto y el central (ver 10.3.3);
- e) análisis total de registros y archivos;
- f) verificaciones para asegurar que los programas de las aplicaciones se ejecutan a la hora correcta;
- g) verificaciones para asegurar que los programas se ejecutan en orden correcta y terminan en caso de una falla, y que además se detiene el procesamiento hasta que se resuelve el problema.

10.2.3 Autenticación de mensaje

La autenticación de mensaje es una técnica que se usa para detectar los cambios no autorizados o una corrupción de los contenidos de un mensaje electrónico transmitido. Se puede implementar por hardware o software, con el apoyo de un dispositivo físico de autenticación de mensaje o de un algoritmo de software.

Se debería considerar la autenticación de mensajes para aplicaciones donde hay un requisito de seguridad para proteger la integridad del contenido del mensaje con alta importancia, por ejemplo, transferencia electrónica de fondos, especificaciones, contratos, propuestas, etc. u otros intercambios similares de datos electrónicos. Se debería realizar una evaluación de los riesgos de la seguridad para determinar si se requiere autenticación del mensaje e identificar el método más apropiado de implementación.

La autenticación de mensaje no está diseñada para proteger los contenidos de un mensaje debido a la divulgación no autorizada. Las técnicas criptográficas (ver 10.3.2 y 10.3.3) se pueden usar como una forma apropiada de implementación de autenticación de mensaje.

10.2.4 Validación de los datos de salida

Los datos de salida de una aplicación del sistema se deberían validar para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias. Típicamente los sistemas se construyen con la premisa que tienen que garantizar una apropiada validación, verificación y prueba, de que la salida siempre será correcta. Esto no siempre es el caso. La validación de la salida puede incluir:

- a) Verificaciones de admisibilidad para probar si los datos de salida son razonables.
- b) Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- c) Proveer suficiente información para el lector o para el sistema de procesamiento subsecuente, para determinar la exactitud, totalidad, precisión y clasificación de la información.
- d) Procedimientos para responder las pruebas de validación de la salida.
- e) Definir las responsabilidades de todo el personal involucrado en el proceso de los datos de salida.

10.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o la integridad de la información.

Se deberían usar técnicas y sistemas criptográficos para la protección de la información que se considera en riesgo y para la cual otros controles no proveen una protección adecuada.

10.3.1 Política en el uso de controles criptográficos

Para tomar una decisión si una solución criptográfica es apropiada, se debería ver como parte del amplio proceso de evaluación de riesgos y de selección de controles. Se debería realizar una evaluación de riesgo para determinar el nivel de protección que se le debería dar a la información. Luego, esta evaluación se puede usar para determinar qué control criptográfico es apropiado, qué tipo de control se debería aplicar y para qué propósito y procesos del negocio.

La organización debería desarrollar una política del uso de controles criptográficos para la protección de su información. Tal política es necesaria para maximizar beneficios y minimizar los riesgos del uso de técnicas criptográficas, y evitar el uso incorrecto e inadecuado. Cuando se desarrolle la política se debería considerar lo siguiente:

- a) enfocar la gestión en el uso de los controles criptográficos en la organización, incluyendo los principios generales bajo los que se debería proteger la información del negocio;

- b) plantear la gestión de claves, incluir métodos para tratar la recuperación de la información encriptada en el caso de claves perdidas, dañadas o comprometidas;
- c) los roles y responsabilidades, por ejemplo, quién es responsable de:
- d) la implementación de la política;
- e) la gestión de las claves;
- f) cómo se determina el nivel apropiado de protección criptográfica;
- g) las normas que se adoptan para la implementación efectiva en toda la organización (qué solución se usa y para qué proceso del negocio).

10.3.2 Encriptación

La encriptación es una técnica criptográfica que se puede usar para proteger la confidencialidad de la información. Se debería considerar para la protección de información crítica y sensible.

En base a la evaluación del riesgo se debería identificar el nivel de protección necesario tomando en cuenta el tipo y calidad del algoritmo de encriptación que se usa y la longitud de las claves criptográficas que se usan.

Cuando se implementa la política criptográfica de la organización, se debería tener en consideración los reglamentos y restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y las emisiones de flujo de información encriptada más allá de la frontera. Además, se debería tener en consideración los controles que aplican a la exportación e importación de tecnología criptográfica (ver también 12.1.6).

Los especialistas opinan que se debería procurar identificar el nivel apropiado de protección, para seleccionar los productos adecuados, que proveerán la protección necesaria y la implementación de un sistema seguro de gestión de clave (ver también 10.3.5). Además, puede ser necesaria la opinión legal relacionada con las leyes y reglamentos que se pueden aplicar a la organización que desea usar la encriptación.

10.3.3 Firmas electrónicas

Las firmas electrónicas proveen una forma de proteger la autenticidad y la integridad de los documentos electrónicos. Por ejemplo, ellas se pueden usar en el comercio electrónico cuando hay necesidad de verificar quién firmó un documento electrónico y verificar si se ha cambiado el contenido del documento electrónico.

Las firmas electrónicas se pueden aplicar a cualquier forma de documento que se procese electrónicamente, por ejemplo, ellas se pueden usar para firmar un pago electrónico, transferencia de fondos, contratos y acuerdos. Las firmas electrónicas se pueden implementar usando la técnica criptográfica en base a un par de claves relacionadas únicamente, donde una clave se usa para crear una firma (la clave privada) y la otra para verificar la firma (la clave pública).

Se debería tener cuidado en proteger la confidencialidad de la clave privada. Esta clave se debería mantener en secreto ya que alguien que tenga acceso a esta clave puede firmar documentos, por ejemplo pagos, contratos, con lo cual falsificar la firma del dueño de esa clave. Además, es importante proteger la integridad de la clave pública. Esta protección se suministra mediante el uso de un certificado de clave pública (ver 10.3.5).

Es necesario tener en consideración el tipo y calidad del algoritmo de firma que se usa y la longitud de las claves que se usan. Las claves criptográficas que se usan para las firmas electrónicas deberían ser diferentes de aquellas que se usan para encriptación (ver 10.3.2).

Cuando se usan firmas electrónicas se debería tener en consideración toda la legislación pertinente que describe las condiciones bajo la cual la firma electrónica es legalmente válida. Por ejemplo, en el caso de comercio electrónico es importante conocer el estado legal de las firmas electrónicas. Puede ser necesario tener contratos válidos u otros acuerdos para apoyar el uso de las firmas electrónicas cuando el marco legal sea inadecuado. La opinión legal debería tener en consideración las leyes y reglamentos que se pueden aplicar a la organización que desea usar las firmas electrónicas.

10.3.4 Servicios de no repudio

Los servicios de no repudio se deberían usar cuando sea necesario resolver las disputas con respecto a la ocurrencia o no de un evento o una acción, por ejemplo, una disputa que involucra el uso de una firma electrónica en un contrato electrónico o pago. Ellos pueden ayudar a establecer la evidencia para substanciar si ha ocurrido un evento particular o una acción, por ejemplo, el rechazo del envío de una instrucción con firma electrónica usando el correo electrónico. Estos servicios se basan en el uso de técnicas de encriptación y de firma electrónica (ver también 10.3.2 y 10.3.3).

10.3.5 Gestión de claves

10.3.5.1 Protección de claves criptográficas

La gestión de claves criptográficas es esencial para el uso efectivo de las técnicas criptográficas. Cualquier compromiso o pérdida de las claves criptográficas puede llevar al compromiso de la confidencialidad, autenticidad y/o integridad de la información. El sistema de gestión debería estar en el sitio apropiado para apoyar a la organización en el uso de los dos tipos de técnicas criptográficas siguientes:

- a) Las técnicas de clave secreta, donde dos o más partes comparten la misma clave y esta clave se usa para encriptar y desencriptar la información. Esta clave tiene que mantenerse en secreto ya que alguien que tenga acceso es capaz de desencriptar toda la información que es encriptada con esa clave, o introducir información no autorizada.
- b) Las técnicas de clave pública, donde cada usuario tiene un par de claves, una clave pública (que puede ser revelada a cualquiera) y una clave privada (que tiene que mantenerse en secreto). Las técnicas de clave pública se pueden usar para encriptación (ver 10.3.2) y para generar las firmas electrónicas (ver 10.3.3).

Todas las claves se deberían proteger de la modificación y destrucción, las claves secretas y privadas necesitan protección de la divulgación no autorizada. Las técnicas criptográficas también se pueden usar para este propósito. Se debería usar protección física para proteger los equipos que se usan para generar, almacenar y archivar las claves.

10.3.5.2 Normas, procedimientos y métodos

Un sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

- a) generar claves con diferentes sistemas criptográficos y diferentes aplicaciones;
- b) generar y obtener los certificados de clave pública;
- c) distribuir claves destinadas a los usuarios, incluyendo cómo se deberían activar las claves cuando se reciban;
- d) almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves;
- e) cambiar o actualizar claves, incluyendo reglas de cuándo y cómo éstas se deberían cambiar;
- f) tratamiento de las claves comprometidas;
- g) revocar claves, incluyendo como las claves se deberían aislar o desactivar, por ejemplo, cuando las claves se hayan comprometido o cuando un usuario deja una organización (en este caso las claves se deberían también archivar);

- h) recuperar claves que se perdieron o se corrompieron como parte de la gestión de continuidad del negocio, por ejemplo, para la recuperación de información encriptada;
- i) archivar claves, por ejemplo; para información archivada o de respaldo;
- j) destruir claves;
- k) registrar y auditar las actividades relacionadas con la gestión de claves.

Con el fin de reducir la probabilidad de compromiso, las claves deberían tener definido los datos de activación y desactivación, de modo que ellas se puedan usar sólo por un período limitado de tiempo. Este período de tiempo debería ser independiente de las circunstancias en las que se usa el control criptográfico y se percibe el riesgo.

Puede ser necesario considerar los procedimientos para el manejo de las exigencias legales para acceder a las claves criptográficas, por ejemplo, puede ser necesario que la información encriptada esté disponible en una forma no encriptada para evidencia en una corte.

Además del hecho de gestionar en forma segura las claves secreta y privada, también se debería considerar la protección de las claves públicas. Existe la amenaza de que alguien falsifique una firma electrónica mediante el reemplazo de una clave pública de usuario por la propia. Este problema es atendido con el uso de un certificado de clave pública. Estos certificados se deberían generar de manera que únicamente relacionen la información con el dueño del par de clave pública/privada de la clave pública. Por lo tanto es importante que el proceso de gestión que genera estos certificados pueda ser de confianza. Este proceso normalmente lo realiza una autoridad de certificación que podría ser una organización reconocida con controles y procedimientos apropiados en el sitio para proveer el grado de confianza necesario.

Los contenidos de los acuerdos a nivel de servicios o contratos con proveedores externos de servicios de criptografía, por ejemplo, con una autoridad de certificación, deberían cubrir las materias de responsabilidad y confiabilidad de servicios y tiempos de respuesta para el suministro de ellos (ver 4.2.2).

10.4 Seguridad de los archivos de sistema

Objetivo: Asegurar que los proyectos de Tecnología de la Información (TI) y las actividades de apoyo se conduzcan de manera segura. Se debería controlar el acceso a los archivos del sistema.

El mantenimiento de la integridad del sistema debería ser responsabilidad de la función de usuario o del grupo de desarrollo a quienes pertenece el software o la aplicación del sistema.

10.4.1 Control del software operacional

Se debería proveer control para la implementación del software operacional de los sistemas. Para minimizar el riesgo de corrupción de los sistemas operacionales, se deberían considerar los controles siguientes:

- a) Realizar la actualización de las bibliotecas de programas operacionales sólo mediante la biblioteca designada por una autorización apropiada de la dirección (ver 10.4.3).
- b) Mantener, si es posible, en los sistemas operacionales sólo los códigos ejecutables.
- c) No implementar los códigos ejecutables en un sistema operacional hasta que se obtenga la evidencia de prueba exitosa y la aceptación del usuario y se hayan actualizado las bibliotecas de programas fuentes.
- d) Mantener una auditoría de registro de todas las actualizaciones de las bibliotecas de programas operacionales.
- e) Guardar las versiones previas del software como una medida de contingencia.

El software suministrado por los proveedores que se usa en los sistemas operacionales se debería mantener como nivel de apoyo. Cualquier decisión para actualizar a una nueva versión de software debería tomar en cuenta la seguridad de la nueva versión, es decir, la introducción de la nueva funcionalidad de seguridad o la variedad y severidad de los problemas de seguridad que afectan esta versión. Los parches de software se deberían aplicar cuando ellos puedan ayudar a reducir o eliminar la deficiencia de seguridad.

Cuando sea necesario los accesos lógicos o físicos sólo se deberían dar a los proveedores para propósitos de apoyo, y con la aprobación de la dirección. Se deberían monitorear las actividades del proveedor.

10.4.2 Protección de los datos de prueba del sistema

Los datos se deberían proteger y controlar. Las pruebas del sistema y la aceptación generalmente requieren volúmenes importantes de datos de prueba que son tan cercanos como sea posible a los datos de operación. Se debería evitar el uso de las bases de datos operacionales que contienen información personal. Si tal información se usa, debería ser despersonalizada antes de su uso. Se deberían aplicar los siguientes controles para proteger los datos operacionales, cuando se usan para propósitos de prueba:

- a) Los procedimientos de control de acceso, que se consideran para las aplicaciones operacionales del sistema, también se deberían aplicar a las pruebas de las aplicaciones del sistema.
- b) Separar la autorización cada vez que la información operacional se copie para una prueba de la aplicación del sistema.

- c) Borrar la información operacional de prueba de la aplicación del sistema inmediatamente después que la prueba se complete.
- d) Registrar la copia y uso de la información operacional para proveer un seguimiento de auditoría.

10.4.3 Control de acceso a la biblioteca de programas fuentes

Con el fin de reducir la corrupción potencial de programas de computadores; se debería mantener un estricto control de los accesos a las bibliotecas de programas fuentes como sigue (ver también 8.3):

- a) Las bibliotecas de programas fuentes, cuando sea posible, no se deberían mantener en los sistemas operacionales.
- b) Para cada aplicación se debería designar una biblioteca de programas.
- c) El personal TI de apoyo no debería tener acceso irrestricto a las bibliotecas de programas fuentes.
- d) Los programas en desarrollo o mantenimiento no se deberían mantener en las bibliotecas de programas fuentes operacionales.
- e) La actualización de bibliotecas de programas fuentes y la emisión de programas fuentes a programadores sólo se debería ejecutar por la biblioteca designada con autorización del directivo de apoyo TI para la aplicación.
- f) La lista de programas se debería mantener en un ambiente seguro (ver 8.6.4).
- g) Se debería mantener una auditoría de registro de todos los accesos a las bibliotecas de programas fuentes.
- h) Se deberían archivar las versiones antiguas de programas fuentes, con una indicación clara de las fechas y horas precisas cuando ellos estuvieron en operación, junto con todo el software de apoyo, control de trabajo, definiciones de datos y procedimientos.
- i) El mantenimiento y copia de bibliotecas de programas fuentes debería estar sujeto a un estricto procedimiento de control de cambios (ver 10.4.1).

10.5 Seguridad en los procesos de desarrollo y apoyo

Objetivo: Mantener la seguridad del software de aplicación del sistema y de la información.

Se deberían controlar estrictamente los ambientes de apoyo y proyecto.

Los directivos responsables de las aplicaciones del sistema también deberían ser responsables por la seguridad del ambiente de apoyo y proyecto. Ellos deberían asegurar que todos los cambios al sistema propuesto se revisen para verificar que ellos no comprometan la seguridad del sistema o del ambiente operacional.

10.5.1 Procedimientos de control de cambios

Con el fin de minimizar la corrupción de los sistemas de información, debería existir un estricto control de la implementación de los cambios. Se deberían exigir los procedimientos formales de control de cambios. Ellos deberían asegurar que los procedimientos de control y la seguridad no se comprometan, que los programadores de apoyo tengan acceso sólo a aquellas partes del sistema necesarias para su trabajo, y que se haya obtenido el acuerdo formal y la aprobación de cualquier cambio. El cambio en el software de aplicación puede impactar el ambiente operacional. Donde sea práctico, se deberían integrar los procedimientos de control de cambios operacionales y de la aplicación (ver también 8.1.2). Este proceso debería incluir:

- a) el mantenimiento de un registro de los niveles de autorización acordados;
- b) el aseguramiento de que los cambios son remitidos por los usuarios autorizados;
- c) la revisión de los procedimientos de integridad y control para asegurar que ellos no se serán afectados con los cambios;
- d) la identificación de todos los software de los computadores, información, entidades de base de datos y hardware que requiere corrección;
- e) la obtención de la aprobación formal de las propuestas detalladas antes de comenzar los trabajos;
- f) el aseguramiento de que el usuario autorizado acepta los cambios antes de cualquier implementación;
- g) el aseguramiento de que la implementación se realiza minimizando la interrupción del negocio;
- h) el aseguramiento de que la documentación del sistema esté actualizada cuando se complete cada cambio y que la documentación antigua se archive o se deseche;
- i) el mantenimiento de un control de la versión de todas las actualizaciones del software;

- j) el mantenimiento de un seguimiento de auditoría de todos los cambios solicitados;
- k) el aseguramiento de que la documentación de operación (ver 8.1.1) y los procedimientos de usuarios se cambien en forma apropiada cuando sea necesario;
- l) el aseguramiento de que la implementación de cambios ocurre en el momento correcto y no perturba el proceso involucrado del negocio.

10.5.2 Revisión técnica de los cambios del sistema operativo

Periódicamente es necesario cambiar el sistema en operación, por ejemplo, instalar una nueva versión del software suministrado o parches. Las aplicaciones del sistema se deberían revisar y probar cuando ocurren cambios, para asegurar que no haya un impacto adverso en la operación o seguridad. Este proceso debería cubrir:

- a) revisar el control de la aplicación y los procedimientos de integridad para asegurar que ellos no se han comprometido por los cambios del sistema en operación;
- b) asegurar que el plan de apoyo anual y el presupuesto cubrirán las revisiones y las pruebas del sistema debidos a los cambios del sistema en operación;
- c) asegurar que la notificación de los cambios del sistema en operación se realiza a tiempo, lo que permite que las revisiones apropiadas se ejecutan antes de la implementación;
- d) asegurar que se hicieron los cambios apropiados a los planes de continuidad del negocio (ver cláusula 11).

10.5.3 Restricción de los cambios a paquetes de software

Las modificaciones a paquetes de software se deberían desalentar. Tanto como sea posible y práctico, el paquete de software suministrado por el vendedor se debería usar sin modificación. Cuando se juzgue esencial modificar un paquete de software, se deberían considerar los puntos siguientes:

- a) el riesgo de que los controles internos y la integridad de los procesos se comprometan;
- b) en todos los casos se debería obtener el consentimiento del vendedor;
- c) la posibilidad de obtener los cambios necesarios desde el vendedor como norma de actualización de programas;
- d) el impacto, producto de los cambios si la organización llega a ser responsable del mantenimiento futuro del software.

Si se juzga que los cambios son esenciales, el software original se debería guardar y los cambios aplicarlos a una copia identificada claramente. Todos los cambios se deberían probar totalmente y documentar, de modo que ellos se puedan reaplicar si es necesario a futuras actualizaciones de software.

10.5.4 Canales encubiertos y código troyano

Un canal encubierto puede exponer información de alguna forma oscura e indirecta. Esto se puede activar por el cambio de un parámetro accesible por los elementos de inseguridad y seguridad de un sistema computacional, o por la incrustación de información en una secuencia de datos. El código troyano se diseña para afectar un sistema de una manera que no está autorizada y no avisa fácilmente y no es requerido por el receptor o usuario del programa. Los canales encubiertos y códigos troyanos raramente ocurren por accidente. Cuando los códigos troyanos o canales encubiertos son una preocupación, se debería considerar lo siguiente:

- a) comprar programas solamente de origen confiable;
- b) comprar programas en código fuente de modo que el código pueda ser verificado;
- c) usar productos evaluados;
- d) inspeccionar todo el código fuente antes del uso operacional;
- e) controlar los accesos y la modificación de los códigos una vez instalados;
- f) usar personal a prueba de confianza para trabajar en sistemas claves;

10.5.5 Desarrollo de software externalizado

Cuando el desarrollo de software es externalizado, se deberían considerar los puntos siguientes:

- a) los convenios de licencias, la propiedad de los códigos y los derechos de propiedad intelectual (ver 12.1.2);
- b) la certificación de la calidad y exactitud del trabajo realizado;
- c) los convenios de resguardos, en el evento de que falle la tercera parte;
- d) los derechos de acceso para auditar la calidad y la exactitud del trabajo hecho;
- e) los requisitos contractuales de la calidad del código;
- f) las pruebas antes de la instalación para detectar código troyano.

11 Gestión de la continuidad del negocio

11.1 Aspectos de la gestión de la continuidad del negocio

Objetivo: Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres.

Se debería implementar un proceso de gestión de la continuidad del negocio para reducir las interrupciones que causan los desastres y fallas de seguridad (los que pueden ser resultado de, por ejemplo, desastres naturales, accidentes, fallas de equipos, y acciones deliberadas) a un nivel aceptable, como una combinación de controles preventivos y recuperativos.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad y pérdidas de servicio. Se deberían desarrollar e implementar planes de contingencia para asegurar que los procesos del negocio se puedan restablecer dentro de una escala de tiempo necesaria. Tales planes se deberían mantener y practicar para que lleguen a ser una parte integral de todos los otros procesos de gestión.

La gestión de la continuidad del negocio debería incluir los controles para identificar y reducir los riesgos, limitar las consecuencias de daños de incidentes y asegurar a tiempo la reanudación de las operaciones esenciales.

11.1.1 Proceso de gestión de la continuidad del negocio

Debería existir un proceso de gestión para desarrollar y mantener la continuidad del negocio de toda la organización. Esto se debería tener junto a los elementos claves de gestión de la continuidad del negocio siguiente:

- a) entender que los riesgos de la organización se enfrentan en términos de su probabilidad y su impacto, incluyendo una identificación y priorización de los procesos críticos del negocio;
- b) entender el impacto que las interrupciones van a tener probablemente en los negocios (esto es importante para las soluciones que se encontrarán para manejar los incidentes menores, como también los incidentes serios que podrían amenazar la viabilidad de la organización), y establecer los objetivos de las instalaciones de procesamiento de la información del negocio;
- c) considerar la contratación de un seguro adecuado que puede formar parte del proceso de continuidad del negocio;
- d) formular y documentar la estrategia de continuidad del negocio, consistente con los objetivos y prioridades acordadas del negocio;
- e) formular y documentar los planes de continuidad del negocio en línea con la estrategia acordada;

- f) probar y actualizar regularmente los planes y procesos ubicados en el sitio;
- g) asegurar que la gestión de continuidad del negocio se incorpora en los procesos y estructura de la organización. La responsabilidad de la coordinación del proceso de gestión de la continuidad del negocio se debería asignar a un nivel apropiado dentro de la organización, por ejemplo, en el comité de seguridad de la información (ver 4.1.1).

11.1.2 Continuidad del negocio y análisis del impacto

La continuidad del negocio debería comenzar con la identificación de los eventos que pueden causar interrupciones a los procesos del negocio, por ejemplo, falla de equipos, inundación y fuego. Esto debería continuar con la evaluación del riesgo para determinar el impacto de aquellas interrupciones (en términos de una escala del daño y período de recuperación). Estas actividades se deberían realizar con el total involucramiento de los dueños de los recursos y procesos del negocio. Esta evaluación considera todos los procesos del negocio, y no está limitada a las instalaciones de procesamiento de información.

Dependiendo de los resultados de la evaluación del riesgo, se debería desarrollar un plan estratégico para determinar la forma de abordar la continuidad del negocio. Una vez que este plan se haya creado, se debería aprobar por la dirección.

11.1.3 Escritura e implementación de los planes de continuidad

Los planes se deberían desarrollar para mantener o restablecer las operaciones del negocio en el tiempo necesario siguiente a la interrupción o falla de algún proceso crítico del negocio. La planificación del proceso de continuidad del negocio debería considerar:

- a) la identificación y acuerdo de todos los procedimientos de emergencia y responsabilidades;
- b) la implementación de los procedimientos de emergencia para permitir la recuperación y restablecimiento en el tiempo requerido. Es necesario dar particular atención a la evaluación de las dependencias externas del negocio y a los contratos existentes;
- c) la documentación de los procesos y procedimientos acordados;
- d) la educación apropiada del personal en los procedimientos y procesos de emergencia acordados, incluyendo una crisis de dirección;
- e) la prueba y actualización de los planes.

El proceso de planificación se debería enfocar en los objetivos requeridos del negocio, por ejemplo, restablecimiento de los servicios específicos de los clientes en un período de tiempo aceptable. Se deberían considerar los servicios y recursos que permitirán esto, incluyendo al personal, recursos de procesamiento de no información, así como configuraciones de recuperación para las instalaciones de procesamiento de información.

11.1.4 Marco de planificación de la continuidad del negocio

Se debería mantener un marco único de los planes de la continuidad del negocio para asegurar que todos los planes sean consistentes y para identificar las prioridades de mantenimiento y pruebas. Cada plan de continuidad del negocio debería especificar claramente las condiciones para su activación, así como las responsabilidades del negocio para ejecutar cada componente del plan. Cuando se identifican nuevos requisitos, por ejemplo, planes de evacuación o cualquier configuración de recuperación existente se deberían corregir, cuando sea apropiado, los procedimientos de emergencia establecidos.

Un marco de planificación de continuidad del negocio, debería considerar lo siguiente:

- a) las condiciones para activar los planes que describen el proceso a seguir (cómo evaluar la situación, quién está involucrado, etc.) antes que cada plan se active;
- b) los procedimientos de emergencia que describen las acciones a ser tomadas después de un incidente que arriesgue las operaciones del negocio y/o la vida humana. Esto debería incluir las disposiciones para la gestión de las relaciones públicas y para la efectiva unión con las autoridades públicas apropiadas, por ejemplo, policía, bomberos y gobierno local;
- c) los procedimientos de recuperación que describan las acciones que se deben tomar para mover las actividades esenciales del negocio o servicios de apoyo a ubicaciones alternativas temporales y colocar en operación los procesos de respaldo del negocio en un tiempo adecuado;
- d) los procedimientos de reanudación que describan las acciones que se deben tomar para volver a las operaciones normales del negocio;
- e) un programa de mantenimiento que especifique cómo y cuándo el plan se probará y el proceso para mantener el plan;
- f) la sensibilización y la educación en las actividades que se diseñan para crear un entendimiento de los procesos de continuidad del negocio y asegurar que los procesos continúan siendo efectivos;
- g) las responsabilidades de los individuos, describiendo quién es el responsable para ejecutar qué componente del plan. Es necesario designar alternativas.

Cada plan debería tener un dueño específico. Los procedimientos de emergencia, el manual de los planes de recuperación y los planes de reanudación deberían estar dentro de la responsabilidad de los propietarios de los recursos y procesos involucrados. Las configuraciones de recuperación de los servicios técnicos alternativos, tales como procesamiento de la información e instalaciones de comunicaciones, generalmente deberían ser de responsabilidad de los proveedores de servicio.

11.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio

11.1.5.1 Pruebas de los planes

Los planes de continuidad del negocio a menudo pueden fallar en las pruebas, debido a suposiciones incorrectas, omisiones o cambios en los equipos o personal. Por lo tanto, estos planes se deberían probar regularmente para asegurar que están actualizados y son efectivos. Tales pruebas deberían asegurar también que todos los miembros del grupo de recuperación y todo el personal pertinente están conscientes de los planes.

El programa de pruebas para el (los) plan(es) de continuidad del negocio debería indicar cómo y cuándo cada elemento del plan se debería probar. Es recomendable probar frecuentemente los componentes individuales del (de los) plan(es). Se debería usar una variedad de técnicas con el fin de proveer seguridad que el (los) plan(es) operará(n) en la vida real. Estas deberían incluir:

- a) pruebas de varios escenarios, tratadas en reunión (discutidas en las configuraciones de recuperación del negocio, usando interrupciones de ejemplo);
- b) simulaciones (particularmente para entrenamiento de las personas en sus roles de gestión post incidente y durante la crisis);
- c) pruebas de recuperación técnica (para asegurar que los sistemas de información efectivamente se puedan restablecer);
- d) pruebas de recuperación en un sitio alternativo (ejecutando los procesos del negocio en paralelo con las operaciones de recuperación desde el sitio principal);
- e) pruebas de las instalaciones y de los servicios del proveedor (para asegurar que los servicios y productos externamente suministrados van a cumplir con el compromiso contratado);
- f) ensayos completos (pruebas que la organización, personal, equipos, instalaciones y procesos puedan salir adelante con las interrupciones).

Estas técnicas las puede usar cualquier organización y deberían reflejar la naturaleza del plan de recuperación específico.

11.1.5.2 Planes de reevaluación y mantenimiento

Los planes de continuidad del negocio se deberían mantener con revisiones y actualizaciones regulares para asegurar su continua efectividad (ver 11.1.5.1 a 11.1.5.3). Los procedimientos deberían incluir el programa de gestión de cambios dentro de la organización para asegurar que las materias de continuidad del negocio sean consideradas apropiadamente.

Se debería asignar la responsabilidad de las revisiones regulares de cada plan de continuidad del negocio; la identificación de los cambios en las disposiciones del negocio que no se reflejan todavía en los planes de continuidad del negocio, debería llevar a una actualización apropiada del plan. Este proceso formal de control de cambio debería asegurar que los planes actualizados se distribuyan y refuerzan debido a las revisiones regulares del plan total.

Ejemplos de situaciones que pueden necesitar planes de actualización incluyendo la adquisición de nuevos equipos, o actualización y cambios de sistemas operacionales:

- a) personal;
- b) direcciones o números telefónicos;
- c) estrategia del negocio;
- d) ubicación de las instalaciones y recursos;
- e) legislación;
- f) personal externo, proveedores y clientes claves;
- g) procesos nuevos o eliminados;
- h) riesgo (operacional y financiero).

12 Cumplimiento

12.1 Cumplimiento con los requisitos legales

Objetivo: Evitar violaciones a cualquier ley civil y criminal, estatutaria, u obligaciones contractuales o reguladoras y a cualquier requisito de seguridad.

El diseño, operación, uso y gestión de los sistemas de información puede estar sujeto a requisitos contractuales de seguridad, reguladores y estatutarios.

Se debería obtener una opinión de los asesores legales de la organización sobre los requisitos legales específicos, o de los profesionales calificados apropiados. Los requisitos legislativos varían de país en país y también varían para la información creada en un país que es transmitida a otro país (es decir el flujo de datos más allá de la frontera).

12.1.1 Identificación de la legislación aplicable

Todos los requisitos pertinentes a lo estatutario, regulatorio y contractual deberían estar explícitamente definidos y documentados para cada sistema de información. Similarmente los controles específicos y las responsabilidades individuales para cumplir con estos requisitos se deberían definir y documentar.

12.1.2 Derechos de propiedad intelectual (DPI)

12.1.2.1 Derechos de autor

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento con las restricciones legales en el uso del material en relación a quien puede tener los derechos de propiedad intelectual, tal como el derecho de autor, derechos de diseño, marca registrada. El infringir el derecho de autor puede llevar a acciones legales que pueden involucrar procedimientos criminales.

Los requisitos legislativos, regulatorios y contractuales pueden colocar restricciones en el copiado de material propietario. En particular, ellos pueden exigir que sólo se pueda usar el material que desarrolla la organización o que está con licencia o suministrado por el desarrollador para la organización.

12.1.2.2 Derechos de autor del software

Los productos de software propietarios generalmente se suministran bajo una licencia de acuerdo que limita el uso del producto a máquinas específicas y puede limitar el copiado a la creación de copias de respaldo solamente. Se deberían considerar los controles siguientes:

- a) publicar la política de cumplimiento con los derechos de autor del software, que define su uso legal y de los productos de información;
- b) emisión de normas de los procedimientos para la adquisición de productos de software;
- c) mantenimiento de la sensibilización de la política de adquisición y derechos de autor del software, e informar de la intención de tomar medidas disciplinarias en contra del personal que viole esto;
- d) mantener un apropiado registro de bienes;
- e) mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.;
- f) implementar controles para asegurar que el número máximo de usuarios permitidos no se exceda;
- g) realizar verificaciones de que sólo el software autorizado y los productos con licencia están instalados;
- h) proveer una política para el mantenimiento apropiado de las condiciones de la licencia;

- i) proveer una política para desechar o transferir el software a otros;
- j) usar herramientas apropiadas de auditoría;
- k) cumplir con los términos y condiciones para el software e información que se obtiene de redes públicas (ver también 8.7.6).

12.1.3 Salvaguardia de los registros de la organización

Los registros importantes de una organización se deberían proteger de pérdidas, destrucción y falsificación. Puede ser necesario que algunos registros se retengan en forma segura para cumplir con los requisitos estatutarios o reguladores, así como para apoyar las actividades esenciales del negocio. Ejemplos de estos registros son los que se pueden requerir como evidencia de que una organización opera dentro de las reglas estatutarias o reguladoras, para asegurar una defensa adecuada en acciones civiles o criminales, o para confirmar el estado financiero de una organización con respecto a la casa matriz, socios y auditores. El período de tiempo y el contenido de los datos de la información que se retiene se puede fijar por una ley o un reglamento.

Los registros se deberían clasificar en tipos de registro, por ejemplo, registros contables, registros de base de datos, registros de transacciones, registros de auditoría y procedimientos operacionales, cada uno con detalles de períodos de retención y tipo de dispositivo de almacenamiento, por ejemplo, papel, microficha, magnético, óptico. Cualquier clave criptográfica relacionada, asociada con los archivos encriptados o firmas electrónicas (ver 10.3.2 y 10.3.3), se debería mantener en forma segura y estar disponible a las personas autorizadas cuando sea necesario.

Se debería tener en consideración la posibilidad de degradación de los dispositivos que se usan para almacenar los registros. Se deberían implementar los procedimientos de almacenamiento y manipulación de acuerdo con las recomendaciones del fabricante.

Cuando se elijan los dispositivos de almacenamiento electrónico, se deberían incluir procedimientos para asegurar la capacidad de acceder a los datos (dispositivo y formato que se pueda leer) en todo el período de retención, para salvaguardar la pérdida debido a cambios futuros de tecnología.

Los sistemas de almacenamiento de datos se deberían elegir de modo que los datos necesarios se puedan recuperar de manera aceptable para un tribunal, por ejemplo, todos los registros requeridos se puedan recuperar en un marco de tiempo aceptable y en un formato aceptable.

El sistema de almacenamiento y manipulación debería asegurar una clara identificación de registros y su período de retención estatutario y regulador. Se debería permitir una destrucción apropiada de registros después de este período, si ellos no son necesarios en la organización.

Para cumplir estas obligaciones, los siguientes pasos se deberían tomar dentro de la organización:

- a) Se deberían emitir guías para retener, almacenar, manipular y desechar registros e información.
- b) Se debería elaborar un cronograma para guardar e identificar los tipos de registro esenciales y el período de tiempo durante el cual ellos se deberían retener.
- c) Se debería mantener un inventario de las fuentes de las claves de información.
- d) Se deberían implementar controles apropiados para proteger los registros esenciales y la información de pérdidas, destrucción y falsificación.

12.1.4 Protección de los datos y de la privacidad de la información personal

Diversos países han introducido en la legislación controles adecuados en el procesamiento y transmisión de datos personales (generalmente la información de las personas que se pueden identificar de esa información). Tales controles pueden imponer obligaciones a aquellos que reúnen, procesan y diseminan la información personal, y puede restringir la capacidad de transferir esos datos a otros países.

El cumplimiento con la legislación a la protección de datos, requiere un control y una estructura de gestión adecuada. A menudo esto se logra mejor con la designación de un funcionario de protección de datos quien debería proveer una guía a los directivos, usuarios y proveedores de servicios de sus responsabilidades individuales y de los procedimientos específicos que se deberían seguir. Debería ser responsabilidad de los dueños de los datos informar al funcionario de protección de datos en relación a cualquier propuesta para mantener la información personal en un archivo estructurado, y asegurar el conocimiento de los principios de protección de datos definidos en la legislación pertinente.

12.1.5 Prevención del mal uso de las instalaciones de procesamiento de la información

Las instalaciones de procesamiento de la información de una organización se proveen para propósitos del negocio. La dirección debería autorizar su uso. Cualquier uso de estas instalaciones para propósitos no autorizados o no del negocio, sin la aprobación de la dirección, se debería considerar como uso impropio de las instalaciones. Si tal actividad se identifica por monitoreo u otros medios, esto debería llamar la atención del directivo para que tome una acción disciplinaria apropiada.

La legalidad del uso del monitoreo varía de país en país y puede ser necesario notificar a los empleados de tales monitoreos u obtener su acuerdo. Se debería tomar en cuenta el marco legal antes de implementar los procedimientos de monitoreo.

Muchos países tienen o están en proceso de introducir leyes para protegerse del mal uso de los computadores. Puede ser un delito criminal usar un computador para propósitos no autorizados. Por lo tanto es esencial que todos los usuarios tengan conciencia del alcance preciso del acceso permitido. Esto se puede lograr, por ejemplo, dando a los usuarios autorización escrita, una copia firmada por ellos se debería guardar en la organización. Los empleados de una organización y los usuarios de terceras partes, deberían ser notificados que no está permitido el acceso, excepto el que esté autorizado.

Al registrarse un usuario se debería presentar en la pantalla del computador un mensaje de advertencia e indicar que el sistema al que se va a entrar es privado y que el acceso no autorizado no está permitido. El usuario toma conocimiento y reacciona apropiadamente al mensaje en la pantalla para continuar con el proceso de registro.

12.1.6 Regulación de los controles criptográficos

Algunos países han implementado acuerdos, leyes, reglamentos u otros instrumentos para controlar el acceso o el uso de controles criptográficos. Tales controles pueden incluir:

- a) importar y/o exportar hardware y software de computadores para realizar las funciones criptográficas;
- b) importar y/o exportar hardware y software que fue diseñado para tener funciones criptográficas agregadas a él;
- c) métodos obligatorios o discrecionales de acceso de los países a la información encriptada por hardware o software para proveer confidencialidad del contenido.

El marco legal se debería procurar para asegurar el cumplimiento con las leyes nacionales. También se debería tomar en cuenta la opinión legal, antes de encriptar la información o antes que los controles criptográficos se transporten a otro país.

12.1.7 Recopilación de evidencias

12.1.7.1 Reglas para la evidencia

Es necesario tener una adecuada evidencia para apoyar una acción en contra de una persona u organización. Cada vez que esta acción sea una materia disciplinaria interna, la evidencia necesaria se describirá mediante los procedimientos internos.

Cuando la acción involucra las leyes, ya sean criminales o civiles, la evidencia que se presente debería estar conforme con las reglas de la evidencia frente a la ley pertinente o con las reglas de la corte específica en la cual el caso se tratará. En general estas reglas cubren:

- a) admisibilidad de la evidencia: es decir si la evidencia puede o no usarse en la corte;

- b) peso de la evidencia: la calidad y totalidad de la evidencia;
- c) evidencia adecuada de que los controles han operado correctamente y consistentemente (es decir, evidencia de control del proceso) en todo el período en que se recuperó, almacenó y procesó la evidencia por el sistema.

12.1.7.2 Admisibilidad de la evidencia

Para alcanzar la admisibilidad de la evidencia, las organizaciones deberían asegurar que sus sistemas de información cumplen con las normas publicadas o los códigos de prácticas para la generación de evidencias admisibles.

12.1.7.3 Calidad e integridad de la evidencia

Para alcanzar la calidad y totalidad de la evidencia, es necesario un seguimiento fuerte de la evidencia. En general, tal seguimiento fuerte se puede establecer bajo las siguientes condiciones:

- a) Para documentos en papel: el original se guarda en forma segura y se registra quién lo encontró, dónde lo encontró, cuándo se encontró y quién confirma el descubrimiento. Cualquier investigación debería asegurar que los originales no están falsificados.
- b) Para la información en dispositivos computacionales: se debería tener copia de cualquier dispositivo removible, información en discos duros o en memorias, para asegurar la disponibilidad. El registro de todas las acciones durante el proceso de copia se debería guardar y el proceso se debería confirmar. Se debería guardar en forma segura una copia del dispositivo y el registro.

Cuando se detecta un incidente por primera vez, puede no ser obvio que llevará a una posible acción legal. Por lo tanto, existe el peligro que la evidencia necesaria se destruya accidentalmente antes de que se analice la severidad del accidente. Es aconsejable involucrar tempranamente a un abogado o a la policía en cualquier acción legal contemplada y tomar nota de la evidencia necesaria.

12.2 Revisión de las políticas de seguridad y cumplimiento técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad de la organización.

La seguridad de los sistemas de información se debería revisar regularmente.

Tales revisiones se deberían realizar a las políticas de seguridad apropiadas y a las plataformas técnicas y se deberían auditar los sistemas de información para ver el cumplimiento con las normas de implementación de seguridad.

12.2.1 Cumplimiento con la política de seguridad

Los directivos deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente. Además, se debería considerar que todas las áreas dentro de la organización tengan una revisión regular para asegurar el cumplimiento con las normas y políticas. Esta debería incluir lo siguiente:

- a) los sistemas de información;
- b) los proveedores de sistemas;
- c) los dueños de la información y bienes de información;
- d) los usuarios;
- e) la gestión.

Los dueños de los sistemas de información (ver 5.1) deberían apoyar las revisiones regulares del cumplimiento de sus sistemas con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad. El uso de los sistemas de monitoreo operacional está cubierto en 9.7.

12.2.2 Verificación del cumplimiento técnico

Los sistemas de información se deberían verificar regularmente si cumplen con las normas de implementación de la seguridad. La verificación del cumplimiento técnico involucra el examen de los sistemas operacionales para asegurar que se han implementado correctamente los controles de hardware y software. Este tipo de verificación del cumplimiento necesita de asistencia técnica de especialistas. Esto se debería realizar manualmente (apoyado por herramientas de software apropiadas, si es necesario) por un ingeniero de sistema experimentado, o por un paquete de software automatizado que genere un informe técnico para la interpretación subsecuente de un técnico especialista.

La verificación del cumplimiento también cubre, por ejemplo, las pruebas de penetración, que podrían realizarse por expertos independientes específicamente contratados para este propósito. Esto puede ser útil para detectar vulnerabilidades en el sistema y para verificar cuán efectivo son los controles en prevenir el acceso no autorizado debido a estas vulnerabilidades. Se debería ejercitar la precaución en el caso de una prueba de penetración exitosa que podría llevar a un compromiso de la seguridad del sistema e inadvertidamente aprovechar otras vulnerabilidades.

Cualquier verificación del cumplimiento técnico se debería realizar por o bajo la supervisión de personas competentes y autorizadas.

12.3 Consideraciones sobre la auditoría del sistema

Objetivo: Maximizar la efectividad y minimizar la interferencia a o desde los procesos de auditoría.

Deberían existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría durante las auditorías del sistema.

También se requiere protección para salvaguardar la integridad y prevenir el mal uso de las herramientas de auditoría.

12.3.1 Controles de auditorías de sistema

Los requisitos de auditoría y las actividades que involucran la verificación de los sistemas operacionales se deberían planificar y acordar cuidadosamente, para minimizar el riesgo de interrupción de los procesos del negocio. Se debería observar lo siguiente:

- a) Los requisitos de auditoría se deberían acordar con la dirección apropiada.
- b) El alcance de las verificaciones se debería acordar y controlar.
- c) Las verificaciones se deberían limitar al acceso de lectura solamente del software y de los datos.
- d) El acceso que no sea de sólo lectura de archivos, se debería permitir solamente para copias aisladas de archivos de sistema, que se deberían borrar cuando se complete la auditoría.
- e) Los recursos de TI para realizar las verificaciones deberían estar disponibles e identificados explícitamente.
- f) Los requisitos para el procesamiento adicional o especial se deberían identificar y acordar.
- g) Todos los accesos se deberían monitorear y registrar para tener un seguimiento de referencia.
- h) Todos los procedimientos, requisitos y responsabilidades se deberían documentar.

12.3.2 Protección de las herramientas de auditoría del sistema

Se deberían proteger los accesos a las herramientas de auditoría, es decir, a los software o archivos de datos, para evitar cualquier compromiso o posible mal uso. Tales herramientas se deberían separar de los sistemas operacionales y de desarrollo y no se deberían mantener en bibliotecas de cintas o áreas de usuarios, a menos que se tenga un apropiado nivel de protección adicional.

NORMA CHILENA OFICIAL

NCh 2777.Of2003
ISO/IEC 17799: 2000

INSTITUTO NACIONAL DE NORMALIZACION  INN-CHILE

Tecnología de la información - Código de práctica para la gestión de seguridad de la información

Information technology - Code of practice for information security management

Primera edición : 2003

Descriptores: tecnología de la información, gestión, seguridad de la información, controles de acceso

CIN 35.040

COPYRIGHT © 2003: INSTITUTO NACIONAL DE NORMALIZACION - INN

* Prohibida reproducción y venta *

Dirección : Matías Cousiño N° 64, 6° Piso, Santiago, Chile

Casilla : 995 Santiago 1 - Chile

Teléfonos : +(56 2) 441 0330 • Centro de Documentación y Venta de Normas (5° Piso) : +(56 2) 441 0425

Telefax : +(56 2) 441 0427 • Centro de Documentación y Venta de Normas (5° Piso) : +(56 2) 441 0429

Web : www.inn.cl

Miembro de : ISO (International Organization for Standardization) • COPANT (Comisión Panamericana de Normas Técnicas)