NOTA IMPORTANTE:

ININ/ Oficina Nacional de Normalización

NORMA CUBANA

NC

ISO/IEC 17799: 2007
(Publicada por la ISO en 2005)

TECNOLOGÍA DE LA INFORMACIÓN — CÓDIGO DE BUENAS PRÁCTICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
(ISO/IEC 17799: 2005, IDT)

Information technology — Code of practice for information security management

ICS: 35.040

1. Edición Abril 2007

Oficina Nacional de Normalización (NC) Calle E No. 261 Vedado, Ciudad de La Habana. Cuba. Teléfono: 830-0835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC), es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información, en el que están representadas las siguientes organizaciones:
  - Ministerio de la Informática y las Comunicaciones
  - SEGURMATICA
  - DESOFT
  - Universidad de las Ciencias Informáticas (UCI)
  - Universidad de Villa Clara
  - Ministerio de Ciencia, Tecnología y Medio Ambiente (CITMATEL)
  - Instituto Superior Politécnico José A. Echeverría
  - Ministerio de Salud Pública (Centro de Control Estatal de Equipos Médicos)
  - Oficina de Seguridad de las Redes Informáticas
  - Oficina Nacional de Normalización
- Es una adopción idéntica por el método de traducción de la Norma Internacional ISO/IEC 17799:2005 *Information technology - Code of practice for information security management*

Oficina Nacional de Normalización (NC)
Calle E No. 261, Vedado, Ciudad de La Habana, Habana 4, Cuba.

Impreso en Cuba.

Índice

Prefacio de la Norma Internacional

La ISO (Organización Internacional de Normalización) y la IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización internacional. Los organismos nacionales que son miembros de la ISO o la IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para ocuparse de campos específicos de la actividad técnica. Los comités técnicos de la ISO y la IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en colaboración con la ISO y la IEC, también toman parte en el trabajo.

Las Normas Internacionales se elaboran de acuerdo con las reglas dadas en las Directivas ISO/IEC, Parte 2.

En el campo de las tecnologías de la información, la ISO y la IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1. Los Proyectos de Normas Internacionales adoptados por el Comité Técnico Conjunto son circulados a los organismos nacionales para su votación. La publicación de estos como una Norma Internacional requiere la aprobación de al menos un 75 % de los organismos nacionales que ejerzan el voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta Norma Internacional puedan estar sujetos a derechos de patente. La ISO y la IEC no son responsables de la identificación alguno o todos de esos derechos de patente.

La Norma Internacional ISO/IEC 17799 fue preparada por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnologías de la Información*, subcomité SC 27, Técnicas de seguridad en TI.

Esta segunda edición cancela y remplaza la primera edición (ISO/IEC 17799:2000), la cual ha sido revisada técnicamente.

Una familia de Normas Internacionales sobre Sistema de Gestión de Seguridad de la Información (SGSI) está siendo desarrollada por el ISO/IEC JTC 1/SC 27. La familia de Normas Internacionales incluye normas de requisitos para un sistema de gestión de la seguridad de la información, gestión de riesgos, medición y métricas, y directrices de implementación. Esta familia adoptaría un esquema numérico basado en la serie de números 27000 y subsecuentes.

A partir del año 2007, se ha propuesto incorporar la nueva edición de la norma ISO/IEC 17799 a este nuevo esquema numérico bajo la denominación ISO/IEC 27002.

0. Introducción

0.1 ¿Qué es la seguridad informática?

La información es un activo que, como otros importantes activos de negocio, es esencial al negocio de una organización y requiere en consecuencia una protección adecuada. Esto es especialmente importante en ambientes de negocio cada vez más interconectados. Como consecuencia de esta creciente interconectividad, la información está ahora expuesta a un número mayor y a una variedad más amplia de amenazas y vulnerabilidades (véase también OECD – *Guidelines for the Security on Information Systems and Networks).*

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o por medios electrónicos, mostrada en filmes o hablada en conversación. Cualquiera sea la forma que tome la información o los medios por los que se comparta o almacene, la misma debería ser siempre protegida adecuadamente.

La seguridad informática es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad informática se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados y mejorados cuando fuere necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización. Esto debería hacerse en forma conjunta con otros procesos de la administración del negocio.

0.2 ¿Por qué es necesaria la seguridad informática?

La información y los procesos que la apoyan, los sistemas y las redes son importantes activos de negocios. Definir, alcanzar, mantener y mejorar la seguridad informática puede ser esencial para mantener la competitividad, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus sistemas y redes de información se enfrentan con amenazas de seguridad procedentes de una amplia variedad de fuentes, incluyendo fraudes informáticos, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como códigos malignos y ataques de intrusión o de denegación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad informática es importante tanto para los negocios del sector público como privado, y para proteger infraestructuras críticas. En ambos sectores, la seguridad informática funcionará como un habilitador, por ejemplo, para lograr el gobierno electrónico o el comercio electrónico, y para evitar o reducir riesgos relevantes. La interconexión de redes públicas y privadas y el hecho de compartir recursos de información aumenta la dificultad de alcanzar un control de acceso. La tendencia hacia la informática distribuida ha debilitado la eficacia de un control central y especializado.

Muchos sistemas informáticos no han sido diseñados para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere de una planificación cuidadosa y una atención al detalle. La gestión de la seguridad informática requiere, como mínimo, la participación de todos los empleados de la organización. También pudiera requerir la participación de los accionistas, proveedores, terceras partes, clientes u otros externos. La asesoría especializada de organizaciones externas puede ser necesaria.

0.3 ¿Cómo establecer los requisitos de seguridad?

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

1. La primera fuente procede de la valoración de los riesgos de la organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se estima su posible impacto.

2. La segunda fuente es el conjunto de requisitos legales, estatuarios, normativos y contractuales que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

3. La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

0.4 Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el perjuicio en el negocio, resultante de los fallos de seguridad.

Los resultados de esta evaluación ayudarán a orientar y a determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implementación de los controles seleccionados para proteger contra dichos riesgos.

La evaluación del riesgo debería repetirse periódicamente para tratar cualquier cambio que pudiera influenciar los resultados de la evaluación del riesgo.

Se puede encontrar más información sobre evaluación de riesgos de seguridad en el punto 4.1 “Evaluación de riesgos de seguridad”.

0.5 Selección de controles

Una vez que los requisitos y los riesgos de seguridad han sido identificados y se han tomado las decisiones para el tratamiento de riesgos, deberían elegirse e implantarse los controles apropiados que aseguren la reducción de los riesgos a un nivel aceptable. Los controles pueden elegirse de esta norma o de otro conjunto de controles, o nuevos controles pueden diseñarse para cubrir adecuadamente necesidades específicas. La selección de los controles de seguridad depende de una decisión organizacional basada en los criterios para la aceptación del riesgo, las opciones para el tratamiento del riesgo, y el acercamiento a la gestión general del riesgo aplicado a la organización, y debería también estar conforme a toda la legislación y regulaciones nacionales e internacionales relevantes.

Algunos de los controles en esta norma pueden considerarse como principios rectores para la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Se explican más detalladamente en el siguiente apartado bajo el título "Punto de partida de la seguridad de la información".

Más información sobre seleccionar controles y otras opciones del tratamiento del riesgo se puede encontrar en el apartado 4.2 "Tratando riesgos de seguridad".

0.6 Punto de partida de la seguridad de la información

Un cierto número de controles pueden ser considerados como un buen punto de partida para implementar la seguridad informática. Estos están basados en requisitos legislativos esenciales o que se consideran práctica habitual de la seguridad de la información.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden, dependiendo de la legislación aplicable:

a) la protección de los datos y la privacidad de la información de carácter personal (véase el apartado 15.1.4)
b) la protección de los registros de la organización (véase el apartado 15.1.3)

c) los derechos de la propiedad intelectual (véase el apartado 15.1.2)

Los controles que se consideran práctica habitual para conseguir la seguridad informática, comprenden:

a) la documentación de la política de seguridad informática (véase el apartado 5.1.1)
b) la asignación de responsabilidades de seguridad (véase el apartado 6.1.3)
c) la concienciación, formación y capacitación en seguridad informática (véase el apartado 8.2.2)
d) el correcto procesamiento de las aplicaciones (véase el apartado 12.2)
e) la gestión de la vulnerabilidad técnica (véase el apartado 12.6)
f) la gestión de la continuidad del negocio (véase el apartado 14)
g) la gestión de incidentes de seguridad informática y mejoramiento (véase el apartado 13.2)

Estos controles pueden aplicarse a la mayoría de las organizaciones y en la mayoría de los ambientes.

Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

0.7 Factores críticos de éxito

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implementación de la seguridad informática en una organización:

a) una política de seguridad, objetivos y actividades que reflejen los objetivos del negocio de la organización;
b) un enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) el apoyo visible y el compromiso de la alta dirección;
d) una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) la comunicación eficaz de la necesidad de la seguridad a todos los directivos y empleados;
f) la distribución de directrices sobre la política de seguridad informática de la organización y de normas a todos los empleados y contratistas;
g) proveer recursos para las actividades de gestión de seguridad informática;
h) proveer concientización, formación y educación apropiadas;
i) un proceso efectivo de gestión de incidentes de seguridad de la información;
j) implementación de un sistema de medición[1] utilizado para evaluar el desempeño en la gestión de seguridad informática y las sugerencias de mejoras.

0.8 Desarrollo de directrices propias

Este código de buenas prácticas puede verse como punto de partida para desarrollar directrices específicas de la organización. Pueden no ser aplicables todas las recomendaciones y controles de este código. Incluso pueden requerirse controles y recomendaciones adicionales que este documento no incluye. Cuando sean desarrollados documentos que contengan controles y recomendaciones adicionales, puede ser útil, cuando sea aplicable, mantener referencias cruzadas a los apartados de esta norma que faciliten la realización de pruebas de cumplimiento a los auditores y socios del negocio.

TECNOLOGÍAS DE LA INFORMACIÓN — CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA

1 Alcance

Esta Norma Cubana establece recomendaciones y principios generales para iniciar, implantar, mantener y mejorar la gestión de la seguridad informática en una organización. Los objetivos señalados en esta norma internacional proporcionan recomendaciones generales sobre las metas comúnmente aceptadas para la gestión de la seguridad informática.

Los objetivos de control y los controles de esta norma internacional están pensados para ser implementados a fin de alcanzar los requisitos identificados por una evaluación del riesgo. Esta norma internacional puede servir como recomendación práctica para desarrollar normas de seguridad de la organización y una práctica efectiva de la gestión de la misma, así como ayudar a construir confianza en las actividades entre organizaciones.

2 Términos y definiciones

A los efectos de este documento se aplican los siguientes términos y definiciones:

2.1
activo
aquello que tenga valor para la organización
[ISO/IEC 13335-1:2004]

2.2
control
medio de gestionar el riesgo, incluyendo políticas, procedimientos, recomendaciones, prácticas o estructuras de la organización, que pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA: Control también es usado como sinónimo para salvaguarda o contramedida.

2.3
guía
una descripción que clarifica qué debería ser hecho y cómo, para alcanzar los objetivos establecidos en las políticas.
[ISO/IEC 13335-1:2004]

2.4
recursos de procesamiento de la información
todo sistema de procesamiento de la información, servicio o infraestructura, o las localizaciones físicas que los contienen.

2.5
seguridad informática (seguridad de la información)
preservación de la confidencialidad, integridad y disponibilidad de la información; además pueden también estar implicadas otras características, tales como autenticidad, responsabilidad, no repudio, y confiabilidad.

2.6
evento de seguridad informática
un evento de seguridad informática es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad informática o la falla de salvaguardas, o una situación previamente desconocida que pueda ser relevante para la seguridad.
[ISO/IEC TR 18044:2004]

2.7
incidente de seguridad informática
un incidente de seguridad informática es indicado por un único o una serie de eventos indeseados o inesperados de seguridad informática que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad informática.
[ISO/IEC TR 18044:2004]

2.8
política
intención y dirección general expresada formalmente por la dirección.

2.9
riesgo
combinación de la probabilidad de un acontecimiento y de su consecuencia.
[Guía ISO/IEC 73:2002]

2.10
análisis de riesgos
uso sistemático de la información para identificar fuentes y estimar el riesgo.
[Guía ISO/IEC 73:2002]

2.11
evaluación de riesgos
proceso completo de análisis de riesgos y evaluación de riesgos.
[Guía ISO/IEC 73:2002]

2.12
valoración de riesgos
proceso de comparación de riesgos estimados respecto a los criterios de riesgos dados, para determinar la magnitud del riesgo.
[Guía ISO/IEC 73:2002]

2.13
gestión de riesgos
coordinación de actividades para dirigir y controlar una organización respecto del riesgo.

NOTA: La gestión de riesgos incluye generalmente, evaluación de riesgos, tratamiento de riesgos, aceptación de riesgos y comunicación de riesgos.
[Guía ISO/IEC 73:2002]

2.14
tratamiento de riesgos
proceso de selección e implementación de medidas para modificar el riesgo.
[Guía ISO/IEC 73:2002]

2.15
tercera parte
persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión.
[Guía ISO/IEC 2:1996]

2.16
amenaza
una causa potencial de un incidente indeseado, que puede dar lugar a daños a un sistema o a una organización.

[ISO/IEC 13335-1:2004]

2.17
vulnerabilidad
una debilidad de un activo o de un grupo de activos que puede ser explotada por una o más amenazas
[ISO/IEC 13335-1:2004]

3 Estructura de esta norma

Esta norma contiene 11 cláusulas de control de la seguridad que en su conjunto contienen un total de 39 categorías principales de seguridad y una cláusula introductoria a la evaluación y tratamiento de riesgos.

3.1 Cláusulas

Cada cláusula contiene un número de categorías principales de seguridad. Estas once cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cada cláusula) son:

a) Política de Seguridad (1);

b) Organización de la Seguridad de la Información (2);

c) Gestión de Activos (2);

d) Seguridad de Recursos Humanos (3);

e) Seguridad Física y del Ambiente (2);

f) Gestión de Comunicaciones y Operaciones (10);

g) Control de Acceso (7);

h) Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información (6);

i) Gestión de Incidentes de la Seguridad de la Información (2);

j) Gestión de la Continuidad del Negocio (1);

k) Cumplimiento (3).

NOTA: El orden de las cláusulas en esta norma no implica su importancia. Dependiendo de las circunstancias, todas las cláusulas podrían ser importantes, por lo tanto cada organización que aplica esta norma debería identificar las cláusulas aplicables, qué tan importantes son y su aplicación a los procesos individuales del negocio. Todas las listas en esta norma tampoco están en orden de prioridad a menos que esté precisado.

3.2 Categorías principales de seguridad

Cada categoría principal de seguridad contiene:

a) una indicación del objetivo de control que debería alcanzarse; y

b) uno o más controles que se pueden aplicar para alcanzar el objetivo de control.

La descripción del control se estructura de la siguiente manera:

Control

Define la declaración del control específico para satisfacer el objetivo de control.

Guía de implementación

Proporciona información más detallada para apoyar la implementación del control y alcanzar el objetivo de control. Alguna de estas recomendaciones puede no ser conveniente en todos los casos, por lo que pueden ser más apropiadas otras maneras de implementar el control.

Información adicional

Proporciona información adicional que puede necesitar ser considerada, por ejemplo las consideraciones legales y las referencias a otras normas.

4 Evaluación y tratamiento de riesgos

4.1 Evaluando el riesgo de seguridad

Las evaluaciones de riesgo deben identificar, cuantificar, y priorizar los riesgos contra los criterios para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben dirigir y determinar la apropiada acción de gestión y las prioridades para gestionar los riesgos de la seguridad de la información y para implementar los controles seleccionados como protección ante estos riesgos. El proceso de evaluación de riesgos y de selección de controles puede requerir ser realizado repetidas veces de manera de cubrir diversas partes de la organización o de los sistemas de información individuales.

La evaluación de riesgos debería incluir el enfoque sistemático para la estimación de la magnitud de los riesgos (análisis de riesgos) y el proceso de comparación de los riesgos estimados contra los criterios de riesgos para determinar la importancia de los mismos (evaluación de riesgos).
Las evaluaciones de riesgos también deberían realizarse periódicamente para tratar cambios en los requisitos de la seguridad y en la situación del riesgo, por ejemplo, en los activos, las amenazas, las vulnerabilidades, los impactos, la valoración del riesgo, y cuando ocurran cambios significativos. Estas evaluaciones de riesgo se deben emprender de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación de riesgo de la seguridad de la información debería tener un alcance claramente definido para ser eficaz y debería incluir, si es apropiado, relaciones con evaluaciones de riesgo en otras áreas.

El alcance de una evaluación de riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema, o servicios donde esto sea factible, realista, y provechoso. Ejemplos de metodologías de evaluación de riesgo se discuten en ISO/IEC TR 13335-3 (Guía para la gestión de la seguridad de TI: Técnicas para la gestión de la seguridad de TI).

4.2 Tratando los riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si los riesgos pueden ser aceptados o no. Los riesgos pueden ser aceptados si, por ejemplo, se determina que el riesgo es bajo o que el costo del tratamiento no es rentable para la organización. Tales decisiones deberían ser registradas.

Para cada uno de los riesgos identificados siguiendo la evaluación de riesgo una decisión sobre el tratamiento del riesgo necesita ser tomada. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicación de controles apropiados para reducir los riesgos;

b) aceptando riesgos objetivamente y bajo conocimiento, siempre que satisfagan claramente la política y los criterios de la organización para la aceptación del riesgo;
c) evitando riesgos, no permitiendo las acciones que harían ocurrir los riesgos;

d) transfiriendo los riesgos asociados a otras partes, por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del mismo haya sido aplicar controles apropiados, estos deberían seleccionarse e implantarse de manera de alcanzar los requisitos identificados por una evaluación de riesgo. Los controles deberían asegurar que los riesgos son reducidos a un nivel aceptable teniendo en cuenta:

a) requisitos y restricciones de la legislación y de las regulaciones nacionales e internacionales;

b) objetivos de la organización;

c) requisitos y restricciones operacionales;

d) costo de la implementación y de la operación en lo referente a los riesgos que son reducidos, y el remanente proporcional a los requisitos y a las restricciones de la organización;

e) la necesidad de balancear la inversión en la implementación y la operación de controles contra el daño probable como resultado de fallas de la seguridad.

Los controles pueden seleccionarse de esta norma o de otro conjunto de controles, o nuevos controles pueden diseñarse para resolver las necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todos los sistemas de información o ambientes, y puede no ser práctico para todas las organizaciones. Como ejemplo, en 10.1.3 describe cómo las tareas pueden segregarse para prevenir fraudes y errores. Puede que en organizaciones más pequeñas no sea posible segregar todas las tareas y pueden ser necesarias otras maneras de alcanzar el mismo objetivo de control. Como otro ejemplo, en 10.10 describe como el uso del sistema puede ser supervisado y las evidencias ser recogidas. Los controles descritos, por ejemplo, el registro de eventos, puede estar en conflicto con la legislación aplicable, tal como la protección de la privacidad de los clientes o el registro del lugar de trabajo.

Los controles de seguridad de la información deberían considerarse en las etapas de especificación de requisitos y de diseño en sistemas y proyectos. El no hacerlo puede dar lugar a costos adicionales y a soluciones menos eficaces, y quizá, en el peor de los casos, inhabilidad de alcanzar la seguridad adecuada. Debería tenerse presente que ningún sistema de controles puede alcanzar la seguridad completa, y que acciones adicionales de gestión deberían implementarse para supervisar, evaluar, y mejorar la eficiencia y la eficacia de los controles de seguridad para apoyar las metas de la organización.

5 Política de seguridad

5.1 Política de seguridad informática

OBJETIVO: Proporcionar orientación y apoyo de la dirección para la seguridad informática, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

La dirección debería establecer una orientación clara de la política en línea con los objetivos de negocio y demostrar su apoyo y compromiso a la seguridad informática, publicando y manteniendo una política de seguridad en toda la organización.

5.1.1 Documento de política de seguridad informática

Control

La dirección debería aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes, un documento con la política de seguridad informática.

Guía de implementación

El documento con la política de seguridad de la información debería establecer el compromiso de la dirección y el enfoque de la organización para gestionar la seguridad de la información. El documento con la política debería contener declaraciones respecto de:

a) una definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como mecanismo que permite compartir la información (véase el capítulo de Introducción);

b) una declaración de la intención de la dirección, apoyando los objetivos y principios de la seguridad de la información alineada con las estrategias y objetivos de negocio;

c) un marco para fijar objetivos de control y controles, incluyendo la estructura de la evaluación del riesgo y gestión del riesgo
d) una breve explicación de las políticas de seguridad, principios, normas y requisitos de cumplimiento de particular importancia para la organización, incluyendo:

1) cumplimiento de los requisitos legislativos, reguladores y contractuales;
2) requisitos de educación, formación y concientización en seguridad;
3) gestión de la continuidad del negocio;
4) consecuencias de las violaciones a la política de seguridad de la información;

e) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de los incidentes relativos a la seguridad;

f) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

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

Información adicional

La política de seguridad de la información pudo ser parte del documento con la política general. Si la política de seguridad de la información es distribuida fuera de la organización, se debería tomar especial cuidado para no divulgar información sensible. Información adicional se puede encontrar en ISO/IEC 13335-1:2004.

5.1.2 Revisión de la política de seguridad de la información

Control

La política de seguridad de la información debería revisarse a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas.

Guía de implementación

La política de seguridad de la información debería tener un propietario con responsabilidad de gestión aprobada para el desarrollo, la revisión, y la evaluación de la política de seguridad. La revisión debería incluir la evaluación de las oportunidades de mejora de la política de seguridad de la información de la organización

y el enfoque a la gestión de la seguridad de la información en respuesta a cambios en el ambiente de la organización, a las circunstancias del negocio, a las condiciones legales, o al ambiente técnico.
La revisión de la política de seguridad de la información debería tomar en cuenta los resultados de las revisiones por la dirección. Debería haber procedimientos definidos de la revisión por la dirección, incluyendo un calendario o un período para la revisión. Las entradas para la revisión por la dirección deberían incluir información sobre:

a) retroalimentación de las partes interesadas;

b) resultados de las revisiones independientes (véase el apartado 6.1.8);

c) estado de las acciones correctivas y preventivas (véase los apartados 6.1.8 y 15.2.1);

d) resultados de las anteriores revisiones por la dirección;

e) cumplimiento de la política de seguridad de la información y del desempeño de procesos;

f) cambios que podrían afectar el enfoque de la organización a la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, circunstancias del negocio, disponibilidad de recursos, condiciones contractuales, reguladoras, y legales, o cambios al ambiente técnico;

g) tendencias relacionadas con las amenazas y las vulnerabilidades;

h) incidentes de seguridad de la información reportados (véase el apartado 13.1);

i) recomendaciones proporcionadas por autoridades relevantes (véase el apartado 6.1.6)

La salida de la revisión por la dirección debería incluir cualquier decisión y acción relacionadas con:

a) mejora del enfoque de la organización a la gestión de la seguridad de la información y a sus procesos;

b) mejora de los objetivos de control y de los controles;

c) mejora en la asignación de recursos y/o responsabilidades.

Debería mantenerse un registro de la revisión por la dirección.

Debería obtenerse la aprobación de la dirección para la política revisada.

6 Organización de la seguridad de la información

6.1 Organización interna

OBJETIVO: Gestionar la seguridad de la información dentro de la organización. Debería establecerse un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La dirección debería aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar y revisar la implementación de la seguridad a través de la organización.

Si es necesario, una fuente de asesoramiento especializada en seguridad de la información debería establecerse y estar disponible dentro de la organización. Contactos con especialistas de seguridad o grupos externos a la organización, incluyendo autoridades relevantes, deberían ser desarrollados para mantenerse al día con tendencias de la industria, seguimiento de normas, y métodos de evaluación y proveer puntos de

enlace adecuados cuando se deban manejar incidentes de seguridad de la información. Un enfoque multidisciplinario hacia la seguridad de la información debería ser impulsado.

6.1.1 Compromiso de la dirección con la seguridad de la información.

Control

La dirección debería apoyar activamente la seguridad dentro de la organización a través de una orientación clara, compromiso demostrado, y la asignación explícita de las responsabilidades de seguridad de la información y su reconocimiento.

Guía de implementación

La dirección debería:

a) asegurar que los objetivos de seguridad de la información son identificados, cumplen los requisitos de la organización y están integrados en los procesos relevantes;

b) formular, revisar y aprobar la política de seguridad de la información;

c) revisar la efectividad de la implementación de la política de seguridad;

d) proveer una orientación clara y apoyo visible hacia las iniciativas de seguridad;

e) proveer los recursos necesarios para la seguridad;

f) aprobar la asignación de los roles específicos y responsabilidades en seguridad de la información a lo largo de la organización;
g) iniciar planes y programas para mantener la concientización en seguridad;

h) asegurar que la implementación de los controles de seguridad de la información es coordinada en toda la organización (véase el apartado 6.1.2).

La dirección debería identificar la necesidad de asesoramiento especializado en seguridad de la información, interno o externo, y revisar y coordinar los resultados de dicho asesoramiento a través de la organización.

Dependiendo del tamaño de la organización, tales responsabilidades podrían ser manejadas por un foro dedicado de dirección o por un cuerpo directivo existente, tal como la junta de directores.

Información adicional

Más información se encuentra disponible en ISO/IEC 13335-1:2004

6.1.2 Coordinación de la seguridad de la información.

Control

Las actividades referentes a la seguridad de la información deberían ser coordinadas por representantes de diferentes partes de la organización con funciones y roles pertinentes.

Guía de implementación

Típicamente, la coordinación de la seguridad de la información debería involucrar la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicativos, auditores y personal de

seguridad, y especialistas con habilidades en áreas tales como seguros, aspectos legales, recursos humanos, TI y gestión de riesgos.
Esta actividad debería:

a) asegurar que las actividades referentes a la seguridad son ejecutadas de acuerdo a la política de seguridad;

b) identificar cómo manejar los no cumplimientos;

c) aprobar metodologías y procesos para la seguridad de la información, por ejemplo, evaluación de riesgo, clasificación de la Información;

d) identificar cambios significativos en las amenazas y la exposición de la información y de las instalaciones de procesamiento de la información a las amenazas;

e) evaluar la adecuación y coordinación de la implementación de los controles de seguridad de la información;

f) promover en forma efectiva la educación, la formación y la concientización en seguridad de la información a través de la organización;

g) evaluar la información recibida de los seguimientos y revisiones de los incidentes de seguridad de la información y las acciones recomendadas en respuesta a los mismos.

Si la organización no utiliza un grupo multidisciplinario separado, por ejemplo, porque dicho grupo no es apropiado dado el tamaño de la organización, las acciones descritas más arriba deberían ser llevadas a cabo por otro cuerpo adecuado de dirección o director individual.

6.1.3 Asignación de responsabilidades sobre seguridad de la información.

Control

Deberían definirse claramente todas las responsabilidades de seguridad de la información.

Guía de implementación

La asignación de las responsabilidades de seguridad de la información debería hacerse de acuerdo con la política de seguridad de la información (véase la cláusula 4). Deberían identificarse claramente las responsabilidades para la protección de los activos individuales y para la ejecución de los procesos específicos de seguridad. Esta responsabilidad debería ser complementada, donde sea necesario, con una guía más detallada para sitios e instalaciones de procesamiento de información específicos. Deberían definirse claramente las responsabilidades locales para la protección de activos y para llevar a cabo procesos específicos de la seguridad, como por ejemplo, el plan de continuidad del negocio.

Individuos con responsabilidades de seguridad asignadas pueden delegar tareas de seguridad a otros. Sin embargo, siguen manteniendo la responsabilidad y deberían poder determinar que cualquier tarea delegada se ha cumplido correctamente.

Deberían establecerse claramente las áreas de las cuales los individuos son responsables, en particular deberían considerarse las siguientes:

a) deberían identificarse y definirse claramente los activos y los procesos de seguridad asociados con cada sistema específico;

b) debería asignarse la entidad responsable de cada activo o proceso de seguridad y documentar los detalles de dicha responsabilidad (véase el apartado 7.1.2);

c) deberían definirse y documentarse claramente los niveles de autorización.

Información adicional

Muchas organizaciones nombran un administrador de seguridad de la información para asumir toda la responsabilidad del desarrollo e implantación de la seguridad y para dar soporte a la identificación de controles.

Sin embargo, la responsabilidad de proporcionar recursos e implantar los controles suele recaer en ciertos directivos. Una práctica habitual consiste en designar un propietario de cada activo de información, que se convierte así, en responsable de su seguridad cotidiana.

6.1.4 Proceso de autorización para instalaciones de procesamiento de información.

Control

Debería definirse e implantarse un proceso de autorización por parte de la dirección para nuevas instalaciones de procesamiento de información.

Guía de implementación

Deberían considerarse las siguientes pautas para el proceso de autorización:

a) las nuevas instalaciones deberían tener una autorización de la dirección apropiada para el usuario, autorizando su propósito y uso. También debería obtenerse la autorización del directivo responsable del mantenimiento del entorno de seguridad del sistema de información local, para asegurar que cumple con todas las políticas y requisitos de seguridad relevantes.

b) se debería comprobar donde sea necesario, que el hardware y el software sean compatibles con los demás dispositivos del sistema.

c) el uso de las instalaciones para procesamiento de información personales o privados por ejemplo, computadoras portátiles, computadoras de uso doméstico u otros dispositivos portátiles, puede causar vulnerabilidades, por lo que deberían identificarse e implementarse medidas de control necesarias.

6.1.5 Acuerdos de confidencialidad

Control

Deberían identificarse y revisarse con regularidad los requisitos para los acuerdos de confidencialidad o de no-divulgación, que reflejan las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o de no-divulgación deberían tratar el requisito de proteger la información confidencial usando términos que puedan hacerse cumplir legalmente. Para identificar los requisitos de los acuerdos de confidencialidad y no-divulgación, deberían considerarse los siguientes elementos:

a) una definición de la información a ser protegida (por ejemplo información confidencial);

b) duración prevista del acuerdo, incluyendo los casos en que sea necesario mantener la confidencialidad indefinidamente;

c) acciones requeridas cuando termina un acuerdo;
d) responsabilidades y acciones de los signatarios para evitar la divulgación no autorizada de la información ("necesidad de saber");

e) propiedad de la información, secretos comerciales y propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial;

f) el uso permitido de la información confidencial, y los derechos del signatario para utilizar información;

g) el derecho de auditar y de supervisar actividades que involucran información confidencial;

h) procesos para la notificación y reporte de divulgación no autorizada o brechas de la información confidencial;

i) términos vinculados a la destrucción o devolución de información cuando cesa un acuerdo; y

j) acciones previstas a tomar en caso de ruptura del acuerdo.

Basándose en los requisitos de seguridad de una organización, puede ser necesario incorporar otros elementos en los acuerdos de confidencialidad y no-divulgación.

Los acuerdos de confidencialidad y no-divulgación deberían cumplir con todas las leyes y regulaciones de la jurisdicción a la cual se aplican (véase el apartado 15.1.1).

Los requisitos de los acuerdos de confidencialidad y no-divulgación deberían ser revisados periódicamente y cuando ocurran cambios que influyan en estos requisitos.

Información adicional

Los acuerdos de confidencialidad y no-divulgación protegen la información de la organización e informan a los signatarios de su responsabilidad para proteger, utilizar, y divulgar la información de forma responsable y autorizada.
Puede haber necesidad por parte de una organización de utilizar diversas formas de acuerdos de confidencialidad o no-divulgación en diferentes circunstancias.

6.1.6 Contacto con autoridades

Control

Deberían mantenerse contactos apropiados con las autoridades relevantes.

Guía de implementación

Las organizaciones deberían tener procedimientos vigentes que especifiquen cuándo y qué autoridades (por ejemplo cumplimiento de leyes, departamento de bomberos, autoridades de supervisión) deben ser contactados, y cómo identificar los incidentes de seguridad los cuales deberían ser reportados en tiempo si se sospecha que están incumpliendo la ley.

Las organizaciones que están siendo atacadas desde Internet pueden necesitar terceras partes externas (proveedores de servicios de Internet u operadores de Telecomunicaciones) para tomar acciones contra la fuente del ataque.

Información adicional

El mantenimiento de dichos contactos puede ser un requerimiento para sustentar la gestión de incidentes de seguridad (apartado 13.2) o el proceso de continuidad del negocio y plan de contingencia (cláusula 14). Los contactos con instituciones reguladoras son también útiles para anticiparse y prepararse para cambios próximos de la ley o regulaciones, los cuales tienen que ser implementados por las organizaciones. Los contactos con otras autoridades incluyen utilitarios, servicios de emergencia, salud y seguridad del personal, por ejemplo, departamento de bomberos (en relación con la continuidad del negocio), proveedores de telecomunicaciones (en relación con las líneas de ruteo y la disponibilidad), proveedores de agua (en relación con las instalaciones de refrigeración para el equipamiento).

6.1.7 Contacto con grupos de interés especial

Control

Deberían mantenerse contactos apropiados con los grupos de interés especial u otros foros especializados en seguridad, así como asociaciones de profesionales.

Guía de implementación

La participación en foros o grupos de interés especial debería considerarse un medio para:

a) incrementar el conocimiento sobre las mejores prácticas y mantenerse al día con la información relevante sobre seguridad;

b) garantizar que la comprensión del ambiente de seguridad de la información es actual y completa;

c) recibir advertencias oportunas de alertas, avisos y parches referidos a ataques o vulnerabilidades;

d) obtener acceso a asesoría especializada sobre seguridad de la información;

e) compartir e intercambiar información sobre nuevas tecnologías, productos, amenazas o vulnerabilidades;

f) proveer puntos adecuados de enlace para el manejo de incidentes de seguridad de la información (véase el apartado 13.2.1).

Información adicional

Pueden establecerse acuerdos para compartir la información de forma de incrementar la cooperación y la coordinación de temas de seguridad. Tales acuerdos deberían identificar los requisitos para la protección de información sensible.

6.1.8 Revisión independiente de la seguridad de la información

Control

El enfoque de la organización hacia la gestión de la seguridad de la información y su implementación (objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) debería ser revisado independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Guía de implementación

La revisión independiente debería ser iniciada por la dirección. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de seguridad.

La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por individuos independientes del área a revisar, por ejemplo, por el cargo de auditoría interna, un gerente independiente o una organización externa especializada en estas revisiones. Los individuos que las llevan a cabo deberían tener la experiencia y habilidades apropiadas.

El resultado de la revisión debería ser registrado y reportado a la dirección que inició la revisión. Estos registros deberían ser mantenidos.

Si la revisión independiente identificara que el enfoque y la implementación de la organización para la gestión de la seguridad de la información son inadecuados o no cumplen con la orientación declarada en el documento de política de seguridad de la información (véase el apartado 5.1.1), la dirección debería definir las acciones correctivas.

Información adicional

El área que los directores deberían revisar regularmente (véase el apartado 15.2.1), también puede ser revisada en forma independiente.

Las técnicas de revisión podrían incluir entrevistas de la dirección, verificación de registros o revisión de los documentos de seguridad. La norma ISO 19011:2002, Directrices para la auditoría de los sistemas de gestión de la calidad y/o ambiental, puede proveer una guía de ayuda para realizar la revisión independiente, incluyendo la definición e implementación del programa de revisión. El apartado 15.3 especifica controles relevantes a la revisión independiente de los sistemas operacionales de información y el uso de las herramientas de auditoría de sistemas.

6.2 Partes externas

OBJETIVO: Mantener la seguridad de la información de la organización y de las instalaciones de procesamiento de información a las que tienen acceso las partes externas, o que son procesadas, comunicadas o gestionadas por éstas.
La seguridad de la información de la organización y de las instalaciones de procesamiento de información no debería verse reducida por la introducción de productos o servicios de externos.
Debería controlarse cualquier acceso a las instalaciones de procesamiento de información de la organización y el procesamiento y comunicación de información por externos.
Cuando el negocio requiera trabajo con externos que pueda implicar acceso a la información de la organización y a las instalaciones de procesamiento de la información, u obtener o proveer un producto o servicio de o para externos, se debería realizar una evaluación de riesgos para determinar implicaciones sobre la seguridad y los controles que requieran. Estos controles deberían definirse y aceptarse en un acuerdo con las partes externas.

6.2.1 Identificación de los riegos relacionados con partes externas

Control

Deberían identificarse los riesgos asociados a la información de la organización y a las instalaciones de procesamiento de la información para los procesos de negocio que involucran partes externas, y deberían implementarse controles apropiados antes de otorgar el acceso.

Guía de implementación

Cuando exista la necesidad de permitir el acceso a partes externas a las instalaciones de procesamiento de información o a la información de la organización, debería realizarse una evaluación de riesgos (véase la

cláusula 4) para identificar los requisitos para los controles específicos. La identificación de los riesgos relacionados con el acceso de partes externas debería tener en cuenta los siguientes aspectos:

a) las instalaciones de procesamiento de la información a los cuales requiere acceso la parte externa;

b) el tipo de acceso que la parte externa tendrá a la información y a las instalaciones de procesamiento de la información, por ejemplo:

1) acceso físico, como ser, las oficinas, salas de computadoras, gabinetes de clasificación;
2) acceso lógico, por ejemplo, a las bases de datos de la organización, sistemas de información;
3) conexión de red entre la red de la organización y la de la parte externa, por ejemplo, conexión permanente, acceso remoto;
4) cuando el acceso es realizado en el sitio (*on-site*) o fuera de él (*off-site*);

c) el valor y la sensibilidad de la información involucrada, y la criticidad para las operaciones de negocio;

d) los controles necesarios para proteger la información que no ha sido prevista que sea accesible por las partes externas;

e) el personal de la parte externa involucrada en el manejo de la información de la organización;

f) cómo la organización o el personal autorizado para acceder pueden ser identificados, la manera de verificar la autorización y cuán seguido es necesario que sea reconfirmada;

g) los diferentes medios y controles empleados por la parte externa cuando almacena, procesa, comunica, comparte e intercambia información;

h) el impacto del acceso denegado a la parte externa cuando lo requiere, y de que la parte externa ingrese o reciba información inexacta o engañosa;

i) prácticas y procedimiento para tratar incidentes de seguridad de la información y daños potenciales, al igual que los términos y condiciones para la continuidad del acceso de la parte externa en el caso de un incidente de seguridad de la información;

j) requisitos legales y reguladores y otras obligaciones contractuales pertinentes a la parte externa que deban ser tenidos en cuenta;

k) cómo los intereses de cualquier otro involucrado (*stakeholders*) pueden ser afectados por los acuerdos.

El acceso de las partes externas a la información de la organización no debería ser proporcionado hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato que defina los términos y condiciones para la conexión o el acceso y el acuerdo de trabajo. Generalmente, todos los requisitos de seguridad resultantes del trabajo con partes externas, o los controles internos deberían reflejarse en el acuerdo con la parte externa (véase los apartados 6.2.2 y 6.2.3).
Debería asegurarse que la parte externa sea consciente de sus obligaciones, y acepte las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información de la organización y de las instalaciones de procesamiento de la información.

Información adicional

La información puede ponerse en riesgo por la inadecuada gestión de la seguridad por medio de las partes externas. Deberían identificarse y aplicarse los controles para administrar el acceso de las partes externas a las instalaciones de procesamiento de la información. Por ejemplo, si hay una necesidad especial de confidencialidad de la información, podrían utilizarse acuerdos de no divulgación.

Las organizaciones pueden enfrentar riesgos asociados con los procesos, la gestión y la comunicación entre las organizaciones si se aplica un alto grado de contratación externa, o cuando hay varias partes externas involucradas.
Los controles 6.2.2 y 6.2.3 cubren diferentes acuerdos con partes externas, incluyendo por ejemplo:

a) proveedores de servicios, como ser proveedores de servicios de Internet (*ISPs*), proveedores de red, servicio telefónico, servicios de mantenimiento y soporte;

b) servicios de seguridad gestionados;

c) clientes;

d) contratación externa de instalaciones y/u operaciones, por ejemplo, sistemas de TI, servicios de recolección de datos, operaciones del centro de llamados;

e) consultores de gestión y de negocios, y auditores;

f) desarrolladores y proveedores, por ejemplo, de productos de software y de sistemas de TI;

g) limpieza, abastecimiento y otros servicios de soporte contratados externamente;

h) personal temporal, colocación de estudiantes y otros cargos de corto plazo ocasionales.

Dichos acuerdos pueden ayudar a reducir los riesgos asociados con las partes externas.

6.2.2 Tener en cuenta la seguridad cuando se trata con clientes

Control

Todos los requisitos de seguridad identificados deberían ser tratados antes de brindarle a los clientes acceso a activos o información de la organización.

Guía de implementación

Los siguientes términos deberían ser considerados para tratar la seguridad antes de brindarle a los clientes acceso a cualquiera de los activos de la organización (dependiendo del tipo y la extensión del acceso brindado, no todos ellos podrían aplicarse):

a) protección de activos, incluyendo:

> 1) procedimiento para proteger los activos de la organización, incluyendo información y software, y gestión de las vulnerabilidades conocidas;
> 2) procedimientos para determinar si se han comprometido en algún momento los activos, por ejemplo, pérdida o modificación de datos;
> 3) integridad;
> 4) restricción en la copia y la divulgación de información;

b) descripción del producto y servicio a ser provisto;

c) las diferentes razones, requisitos y beneficios del acceso del cliente;

d) política de control de acceso, que cubra:

> 1) métodos de acceso permitido, y de control y uso de identificadores únicos tales como identificación de usuario (*IDs*) y contraseñas;

2) un proceso de autorización para el acceso de los usuarios y los privilegios;
3) una declaración de que todo acceso que no es explícitamente autorizado está prohibido;
4) un proceso para revocar los derechos de acceso o interrumpir la conexión entre sistemas;

e) acuerdos para el reporte, la notificación y la investigación de las inexactitudes en la información (por ejemplo de detalles personales), incidentes de seguridad de la información y brechas de seguridad;

f) una descripción de cada servicio que va a estar disponible;

g) el nivel a alcanzar por el servicio y los niveles inaceptables del servicio;

h) el derecho al seguimiento, y revocar cualquier actividad relacionada con los activos de la organización;

i) las responsabilidades respectivas de la organización y del cliente;

j) responsabilidades respecto a asuntos legales y cómo se asegura que los requisitos legales son alcanzados, por ejemplo, legislación de protección de datos, especialmente teniendo en cuenta los diferentes sistemas legales de cada nación si el acuerdo involucra la cooperación con clientes en otros países (véase el apartado 15.1);

k) derechos de propiedad intelectual (DPI) y asignación de derechos de copia (véase el apartado 15.1.2) y la protección de cualquier trabajo en colaboración (véase el apartado 6.1.5).

Información adicional

Los requisitos de seguridad relacionados con el acceso del cliente a los activos de la organización pueden variar considerablemente dependiendo de las instalaciones de procesamiento de la información y de la información a los cuales se tiene acceso. Estos requisitos de seguridad pueden tratarse utilizando acuerdos con el cliente, que contengan todos los riesgos y requisitos de seguridad identificados (véase el apartado 6.2.1).

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que permitan el acceso de una parte externa deberían incluir permisos para la designación de otras partes y las condiciones para su acceso y participación.

6.2.3 Tener en cuenta la seguridad en los acuerdos con terceras partes

Control

Los acuerdos con terceros que involucren acceso, procesamiento, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información, o el agregado de productos o servicios a las instalaciones de procesamiento de información deberían cubrir todos los requisitos pertinentes de seguridad.

Guía de implementación

El acuerdo debería asegurar que no hay malentendidos entre la organización y los terceros. Las organizaciones deberían estar satisfechas en cuanto a la indemnidad de los terceros.

Deberían tenerse en cuenta los siguientes términos para su inclusión en los acuerdos con el fin de satisfacer los requisitos de seguridad identificados (véase el apartado 6.2.1):
a) la política de seguridad de la información;

b) los controles que aseguren la protección del activo, incluyendo:

1) procedimientos para proteger los activos de la organización, incluyendo información, software y hardware;
2) todos los controles y mecanismos de protección física requeridos;
3) controles que aseguren la protección contra software malicioso (véase el apartado 10.4.1);
4) procedimientos para determinar si se han comprometido en algún momento los activos, por ejemplo, pérdida o modificación de información, software y hardware;
5) controles que aseguren el retorno o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo;
6) confidencialidad, integridad, disponibilidad, y cualquier otra propiedad relevante (véase el apartado 2.1.5) de los activos;
7) restricciones a la copia y a la divulgación de información, y uso de acuerdos de confidencialidad (véase el apartado 6.1.5);

c) capacitación de los usuarios y administradores en métodos, procedimientos y seguridad;

d) asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información;

e) disposición para la transferencia de personal, cuando sea apropiado;

f) responsabilidades respecto a la instalación y mantenimiento del hardware y software;

g) una estructura de reportes clara y formatos de reporte convenidos;

h) un proceso claro y especificado para la gestión de cambios;

i) políticas de control de acceso, que cubran:

1) las diferentes razones, requisitos y beneficios de la necesidad del acceso por terceras partes;
2) métodos de acceso permitidos y el control y uso de identificadores únicos, tales como las identificaciones de usuario (IDs) y contraseñas;
3) un proceso de autorización para el acceso de usuario y los privilegios;
4) el requisito de mantener una lista de individuos autorizados a utilizar los servicios habilitados, y cuáles son sus derechos y privilegios respecto a dicho uso;
5) una declaración de que toda autorización cuyo acceso no está explicitado está prohibida;
6) un proceso para la revocación de derechos de acceso o la interrupción de la conexión entre sistemas;

j) las disposiciones para el reporte, la notificación y la investigación de los incidentes de seguridad de la información y las brechas de seguridad, así como violaciones de los requisitos establecidos en los acuerdos;

k) una descripción del productos o servicio a ser provisto, y una descripción de la información a habilitar con su clasificación de seguridad (véase el apartado 7.2.1);

l) el nivel a alcanzar por el servicio y los niveles inaceptables del servicio;

m) la definición de criterios verificables de rendimiento, su seguimiento y reporte;

n) el derecho al seguimiento y a revocar cualquier actividad relacionada con los activos de la organización;

o) el derecho a auditar responsabilidades definidas en el acuerdo, a que dichas auditorías sean realizadas por terceros, y a enumerar los derechos estatutarios de los auditores;

p) el establecimiento de un proceso escalable para la resolución de problemas;

q) requisitos de continuidad del servicio, incluyendo medidas de disponibilidad y confiabilidad, en concordancia con las prioridades de negocio de la organización;

r) las respectivas responsabilidades de las partes en el acuerdo;
s) responsabilidades respecto a asuntos legales y como se asegura que los requisitos legales son alcanzados, por ejemplo, legislación de protección de datos, especialmente teniendo en cuenta los diferentes sistemas legales de cada nación si el acuerdo involucra la cooperación con clientes en otros países (véase el apartado 15.1);

t) derechos de propiedad intelectual (DPI) y asignación de derechos de copia (véase el apartado 15.1.2) y la protección de cualquier trabajo en colaboración (véase el apartado 6.1.5);

u) participación de terceros con subcontratistas, y los controles de seguridad que dichos subcontratistas necesitan implementar;

v) condiciones para la renegociación/término de acuerdos:

1) debería establecerse un plan de contingencia en caso de que cualquier parte desee terminar la relación antes de la finalización de los acuerdos;
2) renegociación de los acuerdos si los requisitos de seguridad de la organización cambian;
3) documentación vigente de las listas de activos, licencias, acuerdos o derechos relacionados con ellos.

Información adicional

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre distintos tipos de terceros. Por lo tanto, debería tenerse cuidado de incluir todos los riesgos y los requisitos seguridad identificados (véase el apartado 6.2.1) en los acuerdos. Cuando sea necesario, los procedimientos y controles requeridos pueden ser expandidos en el plan de gestión de la seguridad.

Si la gestión de la seguridad de la información se contrata externamente, los acuerdos deberían aclarar cómo los terceros garantizarán la seguridad adecuada, tal como lo definió la evaluación de riesgos, cómo será mantenida y cómo será adaptada la seguridad para identificar y tratar los cambios en los riesgos.

Algunas de las diferencias entre la contratación externa y otras formas de provisión de servicio por terceros incluyen cuestiones de responsabilidad, planificación de períodos de transición y potencial interrupción de operaciones durante ese período, acuerdos sobre planificación de contingencias y las debidas solicitudes de revisión, así como la recolección y gestión de información de los incidentes de seguridad. Por lo tanto, es importante que la organización planifique y gestione la transición hacia un acuerdo contratado externamente y tenga procesos adecuados establecidos para la gestión de los cambios y la renegociación / el término de acuerdos.

Los procedimientos para continuar procesando en el caso en que el tercero se vuelva incapaz de brindar sus servicios deberían considerase en el acuerdo para evitar cualquier demora en la disposición de los servicios de reemplazo.

Los acuerdos con terceros también pueden involucrar a otras partes. Los acuerdos que permitan el acceso de terceros deberían incluir permisos para la designación de otras partes y las condiciones para su acceso y participación.

Generalmente, los acuerdos son desarrollados en primer término por la organización. Puede impuesto sobre una organización por un tercero. La organización necesita asegurarse que su propia seguridad no es impactada innecesariamente por los requisitos del tercero estipulados en los acuerdos impuestos.

7 Gestión de activos

7.1 Responsabilidad sobre los activos

OBJETIVO: Implementar y mantener una adecuada protección sobre los activos de la organización.

Todos los activos deberían tener un responsable y debería asignarse un propietario a cada uno de ellos.

Deberían identificarse los propietarios para todos los activos y se debería asignar la responsabilidad del mantenimiento de los controles apropiados. La implementación de controles sobre un activo podría ser delegada por su propietario pero éste continúa manteniendo la responsabilidad por la protección del mismo.

7.1.1 Inventario de activos

Control

Todos los activos deberían ser claramente identificados y debería realizarse y mantenerse un inventario de los activos importantes.

Guía de implementación

La organización debería identificar todos sus activos y documentar la importancia de ellos. El inventario de activos debería incluir toda la información necesaria en caso de tener que recuperar el activo luego de un desastre. Esto incluye tipo de activo, formato, localización, información del respaldo, información de licencias e importancia para el negocio. Este inventario no debería duplicar innecesariamente otros inventarios, pero debería garantizarse que el contenido esté alineado.

Asimismo, la propiedad (véase el apartado 7.1.2) y la clasificación (véase el apartado 7.2) de la información debería ser acordada y documentada para cada uno de los activos. Deberían definirse niveles de protección acordes a la importancia del activo, su relevancia en el negocio y su clasificación en relación a la seguridad. (Más información de cómo valorar los activos para representar su importancia puede ser encontrada en ISO/IEC TR 13335-3)

Información adicional

Existen muchos tipos de activos, incluyendo:

a) información: archivos y bases de datos, contratos y acuerdos, documentación de sistemas, información de investigaciones, manuales de usuario, material de entrenamiento, procedimientos operativos o de soportes, planes de continuidad del negocio, procedimientos de vuelta atrás (*fallback*), pistas de auditoría e información archivada;

b) activos de software: software de aplicación, software de sistemas, herramientas de desarrollo y utilitarios;

c) activos físicos: computadoras, equipos de comunicaciones, medios removibles y otros equipos;

d) servicios: servicios de procesamiento y comunicaciones, servicios generales por ejemplo: calefacción, iluminación, suministro de energía y aire acondicionado;

e) recursos humanos, y su calificación, habilidades y experiencia;

f) intangibles, tales como reputación e imagen de la organización.

Los inventarios de activos ayudan a garantizar que se logra la protección eficaz de los activos pero también pueden ser requeridos para otros propósitos del negocio, como por ejemplo, por razones de salud y

seguridad, financieras o de seguros (gestión de activos). El proceso de compilar un inventario de activos es un prerequisito importante de la gestión de riesgos (véase también Cláusula 4).

7.1.2 Propiedad de los activos

Control

Toda la información y los activos asociados con las instalaciones de procesamiento de la información deberían pertenecer a un propietario[2] designado por la organización.

Guía de implementación

El propietario de un activo debería ser responsable de:

a) asegurar que la información y los activos asociados con las instalaciones de procesamiento de la información son clasificados en forma apropiada;

b) definir y revisar periódicamente restricciones y clasificación del acceso al activo teniendo en cuenta las políticas aplicables de control de acceso.

La propiedad puede ser asignada a:

a) un proceso de negocio;
b) un conjunto definido de actividades;
c) una aplicación;
d) un conjunto definido de datos.

Información adicional

Las tareas rutinarias pueden ser delegadas, por ejemplo, a un guardia que vigile el activo diariamente, pero la responsabilidad continúa siendo del propietario.

En sistemas de información complejos puede resultar útil designar un grupo de activos, los cuales actúan en forma conjunta para proveer una función particular como un “servicio”. En este caso el propietario del servicio es responsable por la entrega del mismo, incluido el funcionamiento de los activos que lo proveen.

7.1.3 Uso aceptable de los activos

Control

Deberían ser identificadas, documentadas e implementadas reglas para el uso aceptable de la información y de los activos asociados con las instalaciones de procesamiento de la información.

Guía de implementación

Todos los empleados, contratistas, y usuarios de terceras partes deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con las instalaciones de procesamiento de la información, incluyendo:

a) reglas para el uso del correo electrónico e Internet (véase el apartado 10.8);

[2] El término propietario identifica un individuo o entidad que ha probado habilidades de gestión para controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo. El término propietario no significa que la persona tiene efectivamente derechos de propiedad sobre el activo.

b) directrices para el uso de dispositivos móviles, especialmente para el uso fuera del la organización (véase el apartado 11.7.1).

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de terceras partes que utilicen o tengan acceso a los activos de la organización, deberían estar conscientes de los límites que existen para el uso de la información y de los activos de la organización asociados con las instalaciones de procesamiento de información, así como de los recursos. Deberían responsabilizarse del uso que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

7.2 Clasificación de la información

OBJETIVO: Asegurar que la información recibe el nivel de protección adecuado.

La información debería clasificarse para indicar la necesidad, prioridades y grado de protección esperado en el manejo de la misma.

La información tiene grados variables de sensibilidad y criticidad. Algunos elementos de información pueden requerir un nivel adicional de protección o un manejo especial. Debería utilizarse un sistema de clasificación de la información para definir un conjunto de niveles de protección adecuados, y comunicar la necesidad de medidas especiales de manejo.

7.2.1 Directrices de clasificación

Control

La información debería clasificarse en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

Guía de implementación

La clasificación de información y otros controles de protección asociados deberían tener en cuenta que el negocio necesita compartir o restringir la información, así como los impactos en el negocio asociados a esas necesidades.

Las directrices de clasificación deberían incluir convenciones para la clasificación inicial y reclasificación a lo largo del tiempo, de acuerdo con políticas predeterminadas de control de acceso (véase el apartado 11.1.1)

Debería ser responsabilidad del propietario del activo (véase el apartado 7.2.1) definir la clasificación del activo, revisarla periódicamente y asegurar que esté actualizada y en el nivel apropiado. La clasificación debería tener en cuanta el efecto de acumulación mencionado en el apartado 10.7.2

Debería considerarse el número de categorías de clasificación y los beneficios obtenidos con su uso. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Debería interpretarse cuidadosamente las etiquetas de clasificación que aparezcan en documentos de otras organizaciones que pueden tener distintas definiciones para etiquetas iguales o similares.

Información adicional

El nivel de protección se asegura mediante el análisis de confidencialidad, integridad y disponibilidad y otros requisitos relativos a la información considerada.

La información suele dejar de tener importancia o criticidad tras cierto tiempo, por ejemplo, cuando se ha hecho pública. Estos aspectos deberían considerarse, puesto que una sobreclasificación conllevaría un gasto adicional innecesario.

Cuando se asignan niveles de clasificación, la consideración de documentos con similares requisitos de seguridad en forma conjunta facilita la tarea de clasificación.

En general, la clasificación dada a la información constituye una forma práctica de determinar la manera que la información debería ser tratada y protegida.

7.2.2 Etiquetado y manejo de la información

Control

Debería desarrollarse e implementarse un conjunto apropiado de procedimientos para el etiquetado y manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

Guía de implementación

Los procedimientos para el etiquetado de la información han de cubrir los activos de información en formato físico y electrónico.

La salida procedente de los sistemas que traten información clasificada como sensible o crítica deberían llevar una etiqueta de clasificación adecuada (en la salida). El etiquetado debería reflejar la clasificación de acuerdo con las reglas establecidas en el apartado 7.2.1. Los elementos a considerar incluyen informes impresos, presentaciones en pantalla, medios de almacenamiento (cintas, discos, CDs), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación deberían definirse procedimientos para el manejo de la información, incluyendo procedimientos seguros de, almacenamiento, transmisión, desclasificación y destrucción. Esto debería incluir los procedimientos para la cadena de custodia y el registro de cualquier evento relevante en cuanto a su seguridad.

Los acuerdos con otras organizaciones que impliquen compartir información deberían incluir procedimientos para identificar la clasificación de dicha información y para interpretar las etiquetas de clasificación de otras organizaciones.

Información adicional

El etiquetado y manejo seguro de la información es un requisito clave para acuerdos que impliquen compartir información. Las etiquetas físicas suelen ser la forma más común de etiquetado. Sin embargo, ciertos activos de información, como los documentos en formato electrónico no pueden marcarse físicamente y hay que usar medios electrónicos de marcado, por ejemplo, desplegando marcas de notificación en la pantalla. En donde el marcado no es posible, pueden aplicarse otras maneras para la clasificación, por ejemplo, por la vía de procedimientos o meta-data.

8 Seguridad ligada a los recursos humanos

8.1 Previo al empleo[3]

[3] Explicación: La palabra "empleo" se utiliza aquí para cubrir todas las diferentes situaciones siguientes: empleo de personas (temporales o a largo plazo), nombramiento de roles de trabajo, cambio de roles de trabajo, asignaciones de contratistas, y la terminación de cualquiera de estos acuerdos.

OBJETIVO: Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades, y que sean aptos para los roles para los cuales están siendo considerados, y para reducir el riesgo de hurto, fraude o mal uso de las instalaciones.

Las responsabilidades de seguridad deberían ser tratadas antes de tomar personal en descripciones adecuadas de tareas y en términos y condiciones de empleo.

Todos los candidatos para el empleo, contratistas y usuarios de terceras partes deberían ser filtrados adecuadamente, especialmente para tareas sensibles.

Usuarios de instalaciones de procesamiento de información, ya sea empleados, contratistas y de terceras partes deberían firmar un acuerdo sobre sus roles y responsabilidades de seguridad.

8.1.1 Roles y responsabilidades

Control

Los roles y responsabilidades de seguridad de usuarios empleados, contratistas y de terceras partes deberían ser definidos y documentados de acuerdo con la política de seguridad de la información de la organización.

Guía de implementación

Los roles y responsabilidades de seguridad deberían incluir la exigencia de:

a) implementar y actuar de acuerdo con las políticas de seguridad de la información de la organización (véase apartado 5.1);

b) proteger los activos de accesos no autorizados, divulgación, modificación, destrucción o interferencia;

c) ejecutar procesos o actividades particulares de seguridad;

d) asegurar que la responsabilidad sea asignada al individuo por acciones tomadas;

e) reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización.

Los roles y responsabilidades de seguridad deberían ser definidos y claramente comunicados a los candidatos al puesto durante el proceso de pre-empleo.

Información adicional

Las descripciones de tareas pueden ser usadas para documentar roles y responsabilidades de seguridad. Los roles y responsabilidades de seguridad para individuos no involucrados vía el proceso de empleo de la organización, por ejemplo, involucrados vía una organización de terceras partes, deberían también ser claramente definidos y comunicados.

8.1.2 Selección

Control

Debería realizarse la verificación de antecedentes en todos los candidatos al empleo, contratistas, y usuarios de terceras partes de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.

Guía de implementación
Los chequeos de verificación deberían tener en cuenta toda la legislación relevante sobre privacidad, protección de datos personales y/o relativa a empleo, y debería, donde sea permitido, incluir lo siguiente:

a) disponibilidad de referencias satisfactorias, por ejemplo, una de negocios y una personal;

b) una comprobación (para integridad y exactitud) del currículum vitae del postulante;

c) confirmación de las calificaciones académicas y profesionales declaradas;

d) comprobación independiente de identidad (pasaporte o documento similar);

e) comprobaciones más detalladas, tales como verificación de crédito o antecedentes criminales.

Cuando una tarea, tanto en un nombramiento inicial o en un ascenso, involucre que la persona tenga acceso a instalaciones de procesamiento de información, y en particular si éstas están manejando información sensible, por ejemplo, información financiera o altamente confidencial, la organización debería también considerar comprobaciones adicionales más detalladas.

Los procedimientos deberían definir criterios y limitaciones para comprobaciones de verificación, por ejemplo, quién es elegible para seleccionar personal, y cómo, cuándo y por qué se han de realizar las comprobaciones de verificación.

Debería también realizarse un proceso de selección para contratistas, y usuarios de terceras partes. Donde los contratistas sean provistos a través de una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para selección y los procedimientos de notificación que ellos necesitan seguir si la selección no ha sido completada o si los resultados ocasionan duda o preocupación. De la misma manera, el acuerdo con terceras partes (véase también el apartado 6.2.3) debería especificar claramente todas las responsabilidades y procedimientos de notificación para selección.

Debería recopilarse la información de todos los candidatos a ser considerados para posiciones dentro de la organización y debería ser manejada de acuerdo con toda legislación apropiada existente en la jurisdicción relevante. Dependiendo de la legislación aplicable, los candidatos deberían ser informados con antelación sobre las actividades de selección.

8.1.3 Términos y condiciones de empleo

Control

Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían acordar y firmar los términos y condiciones de su contrato de empleo, el cual debería declarar las responsabilidades de él y de la organización para la seguridad de la información.

Guía de implementación

Los términos y condiciones de empleo deberían reflejar la política de seguridad de la organización además de aclarar y enunciar:

a) que todos los empleados, contratistas y usuarios de terceras partes a los cuales se le dé acceso a información sensible deberían firmar un acuerdo de confidencialidad o de no-divulgación previamente a ser otorgado el acceso a las instalaciones de procesamiento de información;

b) las responsabilidades y derechos legales de empleados, contratistas y todo otro usuario, como por ejemplo, relativas a derechos de copia o legislación de protección de datos (véase también los apartados 15.1.1 y 15.1.2);

c) responsabilidades para la clasificación de información y gestión de activos de la organización asociados a sistemas y servicios de información manejados por el empleado, el contratista o el usuario de terceras partes (véase también los apartados 7.2.1 y 10.7.3);

d) responsabilidades del empleado, contratista o usuario de terceras partes por el manejo de información recibida de otras organizaciones o partes externas;

e) responsabilidades de la organización para el manejo de información personal, incluyendo información personal creada como resultado o durante el contrato laboral con la organización (véase también el apartado 15.1.4);

f) responsabilidades que se extiendan fuera de las instalaciones de la organización y fuera del horario normal de trabajo, por ejemplo, en el caso de trabajo en el domicilio (véase también los apartados 9.2.5 y 11.7.1);

g) acciones a ser tomadas si el empleado, contratista o usuario de terceras partes desatiende los requisitos de seguridad de la organización (véase también el apartado 8.2.3).

La organización debería asegurar que los empleados, contratistas y usuarios de terceras partes acuerden en los términos y condiciones concernientes a la seguridad de la información apropiada a la naturaleza y extensión de acceso que ellos tendrán a los activos de la organización asociados con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas dentro de los términos y condiciones de empleo deberían continuar por un período definido luego de la finalización del empleo (véase también el apartado 8.3).

Información adicional

Se puede usar un código de conducta para cubrir las responsabilidades de los empleados, contratistas y usuarios de terceras partes referentes a confidencialidad, protección de datos, normas éticas, uso apropiado de los equipos e instalaciones de la organización, además de prácticas honestas esperadas por la organización. Los usuarios contratistas o de terceras partes pueden estar asociados con una organización externa que a su vez puede requerir ingresar en acuerdos contractuales en nombre del individuo contratado.

8.2 Durante el empleo

OBJETIVO: Asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y la pertinencia de la seguridad de la información, de sus responsabilidades y obligaciones, y estén equipados para sustentar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de errores humanos.

Las responsabilidades de la dirección deberían ser definidas para asegurar que la seguridad se aplica a lo largo del empleo de un individuo dentro de una organización.

Debería proveerse a todos los empleados, contratistas y usuarios de terceras partes un nivel adecuado de concientización, educación, y formación en procedimientos de seguridad y en el uso correcto de instalaciones de procesamiento de información, para minimizar los posibles riesgos de seguridad. Debería establecerse un proceso disciplinario formal para manejar brechas de seguridad.

8.2.1 Responsabilidades de la dirección

Control

La dirección debería requerir a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad de acuerdo a las políticas y los procedimientos establecidos por la organización.

Guía de implementación

Las responsabilidades de la dirección deberían incluir asegurar que los empleados, contratistas y usuarios de terceras partes:

a) sean apropiadamente instruidos sobre sus roles y responsabilidades de seguridad antes de que se les otorgue acceso a información sensible o a sistemas de información;

b) se les proporcione orientaciones para hacer constar las expectativas sobre la seguridad de su rol dentro de la organización;

c) sean motivados a cumplir con las políticas de seguridad de la organización;

d) logren un nivel de conciencia sobre seguridad relevante a sus roles y responsabilidades dentro de la organización (véase también el apartado 8.2.2);

e) convengan con los términos y condiciones del empleo, lo cual incluye la política de seguridad de la información de la organización y métodos apropiados de trabajo;

f) continúen teniendo aptitudes y calificaciones apropiadas.

Información adicional

Si los empleados, contratistas y usuarios de terceras partes no son concientizados de sus responsabilidades de seguridad, pueden causar un daño considerable a la organización. El personal motivado es probable que sea más confiable y ocasione menos incidentes de seguridad de la información.

Una gestión pobre puede causar que el personal se sienta subvaluado resultando en un impacto negativo en la seguridad para la organización. Por ejemplo, una gestión pobre puede conducir a negligencias en la seguridad o mal uso potencial de los activos de la organización.

8.2.2 Concientización, educación y formación en seguridad de la información

Control

Todos los empleados de la organización y, donde sea relevante, contratistas y usuarios de terceras partes deberían recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, relevantes para su función laboral.

Guía de implementación

La formación en concientización debería comenzar con un proceso de inducción formal ideado para introducir las políticas y expectativas de la organización antes de otorgar acceso a información o servicios.

La formación en curso debería incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como también formación en el uso correcto de instalaciones de procesamiento de información, como por ejemplo, procedimiento de conexión (*log-on*), uso de paquetes de software e información sobre el proceso disciplinario (véase el apartado 8.2.3).

Información adicional

Las actividades de concientización, educación y formación en seguridad deberían ser adecuadas y relevantes al rol de la persona, responsabilidades y habilidades, y deberían incluir información sobre amenazas conocidas, a quién contactar para consejos sobre seguridad adicionales y los canales apropiados para reportar incidentes de seguridad de la información (véase también el apartado 13.1).

La formación para promover la concientización tiene como objetivo permitir a los individuos reconocer problemas e incidentes de seguridad de la información, y responder de acuerdo a las necesidades de su rol laboral.

8.2.3 Proceso disciplinario

Control

Debería existir un proceso disciplinario formal para empleados que han perpetrado una violación a la seguridad.

Guía de implementación

El proceso disciplinario no debería comenzar sin una verificación previa de que la violación a la seguridad ha ocurrido (véase también el apartado 13.2.3 por recolección de evidencia).

El proceso disciplinario formal debería asegurar un tratamiento correcto y justo para los empleados de los cuales se sospecha que han violado la seguridad. El proceso disciplinario formal debería proveer una respuesta graduada que tome en consideración factores tales como la naturaleza y gravedad de la violación y su impacto en el negocio, si es la primera ofensa o una repetición, si el violador fue apropiadamente entrenado, legislación relevante, contratos del negocio y otros factores que se requieran. En casos serios de mal comportamiento el proceso debería permitir remoción instantánea de tareas, derechos de acceso y privilegios, e inmediata escolta fuera del sitio, si es necesario.

Información adicional

El proceso disciplinario debería también ser usado como disuasión para prevenir que los empleados, contratistas y usuarios de terceras partes violen las políticas y procedimientos de seguridad organizacionales, y cualquier otra violación de seguridad.

8.3 Finalización o cambio de la relación laboral o empleo

OBJETIVO: Asegurar que los empleados, contratistas o usuarios de terceras partes se desvinculen de una organización o cambien su relación laboral de una forma ordenada.

Deberían existir responsabilidades para asegurar que la desvinculación de la organización por parte de un empleado, contratista o usuarios de terceras partes sea gestionada, y que sea completada la devolución de todo equipamiento y la remoción de todos los derechos de acceso.

Los cambios en las responsabilidades y en las relaciones laborales dentro de una organización deberían ser gestionados como la finalización de la respectiva responsabilidad o relación laboral en línea con esta sección, y toda nueva contratación debería ser gestionada como se describe en el apartado 8.1.

8.3.1 Responsabilidades en la desvinculación

Control

Las responsabilidades para realizar la desvinculación o el cambio de la relación laboral deberían ser claramente definas y asignadas.
Guía de implementación

La comunicación de las responsabilidades en la desvinculación debería incluir los requisitos de seguridad y responsabilidades legales en curso y, donde sea apropiado, responsabilidades contenidas dentro de algún acuerdo de confidencialidad (véase el apartado 6.1.5), y los términos y condiciones de empleo (véase el apartado 8.1.3) deberían continuar por un período de tiempo luego de la desvinculación del empleado, contratista o usuario de terceras partes.

Las responsabilidades y deberes válidos aún luego de la desvinculación deberían estar contenidas en el contrato del empleado, contratista o usuario de terceras partes.

Los cambios en las responsabilidades o en la relación laboral deberían manejarse de la misma manera que la desvinculación, y la nueva responsabilidad o relación laboral deberían ser controladas como se describe en el apartado 8.1.

Información adicional

La función de recursos humanos generalmente es responsable por el proceso completo de desvinculación laboral y trabaja junto con el supervisor de la persona que egresa para gestionar los aspectos de seguridad de los procedimientos relevantes. En el caso de un contratista, este proceso de responsabilidad en la finalización puede ser llevado a cabo por una agencia responsable por el contratista, y en el caso de otro usuario esto puede ser gestionado por su organización.

Puede ser necesario informar a los empleados, clientes, contratistas, o usuarios de terceras partes de los cambios en los acuerdos operativos y de personal.

8.3.2 Devolución de activos

Control

Todos los empleados, contratistas y usuarios de terceras partes deberían devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.

Guía de implementación

El proceso de desvinculación debería ser formalizado para incluir la devolución de todo software, documentos corporativos, y equipamiento proporcionados previamente. Otros activos organizacionales tales como: dispositivos móviles de computación, tarjetas de crédito, tarjetas de acceso, software, manuales, e información almacenada en medios electrónicos también deben ser devueltos.
En casos en que el empleado, contratista o usuario de terceras partes compra el equipamiento de la organización o utiliza su equipamiento personal, se deben seguir procedimientos para asegurar que toda información relevante sea transferida a la organización y eliminada de forma confiable del equipamiento (véase también el apartado 10.7.1).

En casos en que el empleado, contratista o usuario de terceras partes tiene un conocimiento que es importante para las operaciones en curso, esa información debería ser documentada y transferida a la organización.

8.3.3 Remoción de derechos de acceso

Control

Los derechos de acceso de todo empleado, contratista o usuario de terceras partes a información e instalaciones de procesamiento de información deberían ser removidos como consecuencia de la desvinculación de su empleo, contrato o acuerdo, o ajustado cuando cambia.

Guía de implementación

Cuando ocurre la desvinculación, los derechos de acceso de un individuo a activos asociados con sistemas y servicios de información deberían ser reconsiderados. Esto determinará si es necesario remover los derechos de acceso. Los cambios en la relación laboral deberían ser reflejados en la remoción de todos los derechos de acceso que no fueron aprobados para el nuevo puesto. Los derechos de acceso que deberían ser removidos o adaptados incluyen acceso físico y lógico, llaves, tarjetas de identificación, instalaciones de procesamiento de información (véase también el apartado 11.2.4), suscripciones, y remoción de toda documentación que los identifique como un miembro actual de la organización. Si el empleado, contratista o usuario de terceras partes conoce contraseñas de claves que permanecen activas, estas deberían ser cambiadas al momento de la desvinculación o cambio de cargo, contrato o acuerdo.

Los derechos de acceso a activos de información e instalaciones de procesamiento de información deberían ser reducidos o removidos antes de que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo tales como:

a) si la desvinculación o cambio es iniciado por el empleado, contratista o usuario de terceras partes, o por la dirección y la razón de la desvinculación;

b) las responsabilidades actuales del empleado, contratista o cualquier otro usuario;

c) el valor de los activos accesibles actualmente.

Información adicional

En ciertas circunstancias los derechos de acceso pueden ser asignados sobre la base de estar disponibles a más personas que la persona que egresa, contratista o usuario de terceras partes, por ejemplo, IDs de grupo. En tal circunstancia, los individuos que egresan deberían ser removidos de toda lista de acceso de grupo y deberían realizarse acuerdos para recomendar a todos los otros empleados, contratistas y usuarios de terceras partes involucrados, que no compartan más la información con la persona que egresa.

En casos que la desvinculación sea iniciada por la dirección, los empleados, contratistas o usuarios de terceras partes contrariados pueden deliberadamente dañar información o sabotear equipamiento de procesamiento de información. En casos de personas que renuncian, podrían estar tentados a recoger información para uso futuro.

9 Seguridad física y del ambiente

9.1 Áreas seguras

OBJETIVO: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.

Las instalaciones de procesamiento de información crítica o sensible de la organización deberían estar ubicadas en áreas seguras y resguardadas por un perímetro de seguridad definido, con barreras de seguridad y controles de acceso apropiados. Deberían estar físicamente protegidas contra accesos no autorizados, daños e interferencias.

La protección provista debería ser proporcional a los riesgos identificados.

9.1.1 Perímetro de seguridad física

Control

Deberían utilizarse perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta o recepcionista) para proteger las áreas que contienen información e instalaciones de procesamiento de información.

Guía de implementación

Se deberían considerar e implementar las siguientes recomendaciones sobre el perímetro de seguridad física, según corresponda:

a) el perímetro de seguridad debería estar claramente definido, la ubicación y la resistencia de cada uno de los perímetros deberían depender de los requisitos de la seguridad de los activos dentro del perímetro y de los resultados de una evaluación de riesgos;

b) el perímetro de un edificio o un lugar que contenga instalaciones de procesamiento de información debería tener solidez física (por ejemplo, no tendrá zonas que puedan derribarse fácilmente); los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados, mediante mecanismos de control, por ejemplo, vallas, alarmas, cerraduras, etc.; puertas y ventanas deberían ser bloqueadas cuando se encuentren descuidadas y se debería considerar protección externa para las ventanas, particularmente en niveles bajos;

c) debería existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio; dicho acceso se debería restringir sólo al personal autorizado.

d) donde sea aplicable, se deberían construir barreras físicas para evitar el acceso físico no autorizado y la contaminación del entorno;

e) todas las puertas contra incendios del perímetro de seguridad deberían tener alarma, ser supervisadas y probadas conjuntamente con las paredes para establecer el nivel requerido de resistencia de acuerdo a las normas regionales, nacionales, e internacionales apropiadas; deberían funcionar de acuerdo con las disposiciones locales de protección contra el fuego de modo de garantizar la seguridad;

f) se deberían instalar sistemas de detección de intrusos adecuados según las normas nacionales, regionales o internacionales y probar regularmente para cubrir todas las puertas externas y ventanas accesibles; las áreas vacantes se deberían alarmar siempre; también se debería proporcionar protección para otras áreas, por ejemplo, sala de computadoras o cuartos de comunicaciones;

g) las instalaciones de procesamiento de información gestionadas por la organización se deben separar físicamente de aquellas gestionadas por terceras partes.

Información adicional

La protección física puede ser alcanzada creando una o más barreras físicas alrededor de las premisas de la organización y de las instalaciones de procesamiento de la información. El uso de múltiples barreras brinda protección adicional, mientras que la falta de una barrera no significa que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina bloqueable, o varios cuartos rodeados por una barrera física continua interna de seguridad. Las barreras adicionales y los perímetros para controlar el acceso físico pueden ser necesarios entre áreas con diferentes requisitos de seguridad dentro del perímetro de seguridad.

Se deberían tener consideraciones especiales de seguridad de acceso físico en los edificios donde funcionan múltiples organizaciones.

9.1.2 Controles de accesos físicos

Controles

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que aseguren el acceso sólo al personal autorizado.

Guía de implementación

Deberían considerarse las siguientes recomendaciones:

a) la fecha y hora de entrada y salida de visitantes deberían ser registradas, y todos los visitantes deberían ser supervisados a menos que su acceso se haya aprobado previamente; el acceso debería ser concedido sólo para propósitos especificados y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia;

b) el acceso a las áreas donde se procesa o se almacena la información sensible debería ser controlado y restringido sólo a las personas autorizadas; y deberían usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (*PIN*), para autorizar y validar el acceso; debería mantenerse una pista auditable de todos los accesos, con las debidas medidas de seguridad;

c) para todos los empleados, contratistas y usuarios de terceras partes así como para todos los visitantes debería requerirse el uso de algún tipo de identificación visible y deberían notificar inmediatamente al personal de seguridad si encuentran a visitantes no acompañados y a cualquier persona que no lleve la identificación visible;

d) debería concederse el acceso restringido del personal de soporte de terceras partes a las áreas seguras o a las instalaciones sensibles de procesamiento de la información sólo cuando sea requerido; este acceso debería ser autorizado y supervisado;

e) los derechos de acceso a las áreas seguras deberían ser regularmente revisados y actualizados, y revocados cuando sea necesario (véase el apartado 8.3.3).

9.1.3 Seguridad de oficinas, despachos e instalaciones

Control

Debería diseñarse y aplicarse la seguridad física para oficinas, despachos e instalaciones.

Guía de implementación

Se deberían considerar las siguientes recomendaciones para asegurar oficinas, despachos, e instalaciones:

a) se deberían tomar en cuenta las regulaciones y normativas relevantes en materia de salud y seguridad;

b) las instalaciones claves se deberían situarse de manera de evitar el acceso público;

c) los edificios deberían ser discretos y dar el mínimo indicio de su propósito, cuando sea posible, sin dar muestras obvias, fuera o dentro del edificio, que identifiquen la presencia de las actividades de procesamiento de la información;

d) los directorios y libros de teléfonos internos que identifican ubicaciones de instalaciones sensibles de procesamiento de la información no deberían ser fácilmente accesibles por el público.

9.1.4 Protección contra amenazas externas y del ambiente

Control

Debería diseñarse y aplicarse medios de protección física contra daños por incendio, inundación, terremoto, explosión, disturbios civiles, y otras formas de desastre natural o artificial.

Guía de implementación

Debería tomarse en consideración cualquier amenaza de seguridad presentada por las instalaciones vecinas, por ejemplo, un incendio en un edificio vecino, agua proveniente de la azotea o en pisos a niveles subterráneos o una explosión en la calle.

Deberían considerarse las siguientes recomendaciones para evitar daños ocasionados por incendios, inundaciones, terremotos, explosiones, disturbios civiles, y por otras formas de desastre natural o artificial:

a) los materiales peligrosos o combustibles deberían almacenarse a una distancia prudente de un área segura. Los suministros a granel tales como los materiales de oficina no deberían almacenarse dentro de un área segura;

b) el equipamiento de reserva y los medios de respaldo deberían localizarse a una distancia prudente para evitar daños producto de un desastre que afecten al emplazamiento principal;

c) debería proporcionarse y colocarse convenientemente el equipo apropiado de lucha contra incendios.

9.1.5 El trabajo en las áreas seguras

Control

Debería diseñarse y aplicarse la protección física y las directrices para trabajar en áreas seguras.

Guía de implementación

Deberían considerarse las siguientes recomendaciones:

a) El personal sólo debería conocer la existencia de un área segura, o de sus actividades, si lo necesitara para su trabajo.

b) Se debería evitar el trabajo no supervisado en áreas seguras tanto por motivos de seguridad como para evitar ocasiones de actividades maliciosas.

c) Las áreas seguras desocupadas deberían estar cerradas y controlarse periódicamente.

d) No debería permitirse la presencia de equipos de fotografía, video, audio u otras formas de registro, salvo autorización expresa.

Los acuerdos para trabajar en áreas seguras incluyen controles para los empleados, los contratistas y los usuarios de terceras partes que trabajan en el área segura, así como otras actividades de terceros que ocurren allí.

9.1.6 Áreas de de acceso público, de entrega y de carga

Control

Los puntos de acceso tales como áreas de entrega y de cargamento y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones deberían controlarse, y si es posible, aislarlos de instalaciones de procesamiento de la información para evitar el acceso no autorizado.

Guía de implementación

Deberían considerarse las siguientes recomendaciones:

a) debería restringirse el acceso al área de depósito desde el exterior únicamente al personal autorizado e identificado;

b) el área debería diseñarse para que los suministros puedan descargarse sin que el personal de depósito tenga acceso a otras zonas del edificio;

c) la puerta externa del área debería estar cerrada cuando la interna esté abierta;

d) el material entrante se debería inspeccionar para evitar posibles amenazas (véase el apartado 9.2.1d) antes de llevarlo a su lugar de utilización;

e) el material entrante debería registrarse de acuerdo con el procedimiento de gestión de activos (véase el apartado 7.1) al entrar en el lugar;

f) cuando sea posible, los envíos entrantes y salientes deberían segregarse físicamente.

9.2 Seguridad del equipamiento

OBJETIVO: Prevenir pérdidas, daños, hurtos o comprometer los activos así como la interrupción de las actividades de la organización.

El equipo debería protegerse contra las amenazas físicas y ambientales.

Es necesaria la protección del equipamiento (incluyendo aquel utilizado fuera del local y la eliminación de la propiedad) para reducir el riesgo de accesos no autorizados a la información y para protegerlo contra pérdidas o daños. Esto también debería considerar la ubicación y la disposición del equipamiento. Se pueden requerir controles especiales para proteger contra amenazas físicas, y para salvaguardar las instalaciones de soporte, tales como el suministro eléctrico y la infraestructura de cableado.

9.2.1 Ubicación y protección del equipamiento

Control

El equipamiento debería ubicarse o protegerse para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.

Guía de implementación

Deberían considerarse las siguientes recomendaciones para proteger el equipamiento:

a) el equipamiento debería situarse de manera de minimizar el acceso innecesario a las áreas de trabajo;

b) las instalaciones de procesamiento de la información que manejan datos sensibles deberían ser colocadas y su ángulo de visión restringido para reducir el riesgo de que la información sea vista por

personas no autorizadas durante su uso, y las instalaciones de almacenamiento aseguradas para evitar el acceso no autorizado;

c) los elementos que requieran protección especial deberían aislarse para reducir el nivel general de protección requerida;

d) se deberían adoptar controles para reducir al mínimo el riesgo de amenazas físicas potenciales, como son: hurto, fuego, explosivos, humo, inundaciones (o falta de suministro de agua), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencia de las comunicaciones, radiación electromagnética, y vandalismo;

e) deberían establecerse pautas para comer, beber, y fumar en proximidad de las instalaciones de procesamiento de la información;

f) las condiciones ambientales, tales como temperatura y humedad, deberían supervisarse para verificar que las mismas no afectan negativamente el funcionamiento de las instalaciones de procesamiento de la información;

g) deberían colocarse pararrayos sobre todos los edificios y deberían aplicarse filtros de protección contra rayos a todas las líneas entrantes de energía y de comunicaciones;

h) debería considerarse el uso de métodos de protección especial, como las cubiertas de teclados, para el equipamiento ubicado en ambientes industriales;

i) debería protegerse el equipamiento que procese información sensible para reducir al mínimo el riesgo de fuga de información debido a filtraciones.

9.2.2 Elementos de soporte

Control

Debería protegerse el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.

Guía de implementación

Todos los elementos de soporte, tales como electricidad, abastecimiento de agua, aguas residuales, calefacción/ventilación, y aire acondicionado, deberían adecuarse para los sistemas que están apoyando. Los elementos de soporte deberían examinarse regularmente y probarse adecuadamente de manera de asegurar su funcionamiento apropiado y reducir cualquier riesgo de mal funcionamiento o falla. Debería proveerse un suministro eléctrico apropiado conforme con las especificaciones del fabricante del equipo.

Se recomienda contar con una fuente de energía ininterrumpida (*UPS*) para asegurar el correcto apagado o el funcionamiento continuo del equipamiento que soporta las operaciones críticas del negocio. Los planes de contingencia energéticos deberían contemplar las acciones a tomar en caso de falla de la UPS. Debería tenerse en cuenta el empleo de un generador de reserva si el procesamiento ha de continuar en caso de una falla prolongada en el suministro eléctrico. Debería disponerse de un adecuado suministro de combustible para asegurarse que el generador pueda funcionar por un período prolongado. Los equipos de UPS y los generadores deberían inspeccionarse regularmente para asegurar que tienen la capacidad requerida y probarlos de acuerdo con las recomendaciones del fabricante. Además, se podría considerar el uso de fuentes de energía múltiples o, si el sitio es grande, una subestación energética separada.

Los interruptores de emergencia deberían situarse cerca de las salidas de emergencia en las salas donde se encuentra el equipamiento a fin de facilitar un corte rápido de la energía en caso de producirse una situación

crítica. Se debería proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

El suministro de agua debería ser estable y adecuado para abastecer los sistemas de aire acondicionado, de humectación y de supresión del fuego (cuando sean utilizados). El mal funcionamiento del sistema de abastecimiento de agua puede dañar el equipamiento o evitar que la supresión del fuego actúe con eficacia. Si es requerido debería evaluarse e instalarse un sistema de alarma para detectar un mal funcionamiento en los elementos de soporte.
El equipamiento de telecomunicaciones debería conectarse con el proveedor al menos a través de dos rutas distintas para prevenir fallas en el servicio de una de las rutas de conexión imposibilitando los servicios de voz. Los servicios de voz deberían adecuarse para alcanzar los requisitos legales locales para comunicaciones de emergencia.

Información adicional

Como opción para alcanzar la continuidad en el suministro energético se pueden incluir redes múltiples de alimentación a fin de evitar un único punto de falla en el suministro.

9.2.3 Seguridad en el cableado

Control

Debería protegerse contra interceptación o daños el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información.

Guía para la implementación

Deberían considerarse las siguientes recomendaciones para la seguridad en el cableado:

a) las líneas de energía y telecomunicaciones en instalaciones de procesamiento de la información deben ser subterráneas, siempre que sea posible, o sujetas a una adecuada protección alternativa;

b) el cableado de red debería estar protegido contra interceptación no autorizada o daño, por ejemplo, mediante el uso de conductos o evitando trayectos que atraviesen áreas públicas;

c) los cables de energía deben estar separados de los cables de comunicaciones para evitar interferencias;

d) deberían utilizarse marcas claramente identificables en cables y equipamiento para reducir al mínimo los errores de manejo, tales como conexiones accidentales erróneas de los cables de red;

e) debería utilizarse una lista documentada de las conexiones para reducir la posibilidad de errores;

f) entre los controles adicionales a considerar para los sistemas sensibles o críticos se encuentran los siguientes:

1) instalación de conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección;
2) uso de rutas y/o medios de transmisión alternativos que proporcionen una adecuada seguridad;
3) uso de cableado de fibra óptica;
4) uso de escudos electromagnéticos para proteger los cables;
5) iniciar barridos técnicos e inspecciones físicas contra dispositivos no autorizados conectados a los cables.
6) acceso controlado a los paneles de conexión y a las salas de cable;

9.2.4 Mantenimiento del equipamiento

Control

El equipamiento debería mantenerse adecuadamente para asegurar su continua disponibilidad e integridad.

Guía de implementación

Deberían considerarse las siguientes recomendaciones para el mantenimiento del equipamiento:

a) el equipamiento debería mantenerse de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del proveedor;

b) sólo el personal de mantenimiento debidamente autorizado debería realizar reparaciones y realizar el mantenimiento a los equipos;

c) se deberían mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo;

d) deberían implementarse controles apropiados cuando el equipamiento sea dispuesto para mantenimiento, considerando si este mantenimiento es realizado por personal interno o externo a la organización; la información sensible debería ser removida del equipo, cuando sea necesario, o el personal de mantenimiento debería ser suficientemente transparente;

e) debería cumplirse con todos los requisitos impuestos por pólizas de seguros.

9.2.5 Seguridad del equipamiento fuera de las instalaciones de la organización

Control

Debería asegurarse todo el equipamiento fuera de los locales de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Guía de implementación

El uso de equipamiento destinado al procesamiento de información, fuera de las instalaciones de la organización, debería ser autorizado por la dirección, sin importar quién sea su propietario.

Deberían considerarse las siguientes recomendaciones para la protección del equipamiento fuera de los locales de la organización:

a) los equipos y soportes que contengan datos con información y sean sacados de su entorno habitual no deberían dejarse desatendidos en sitios públicos; cuando viajen, las computadoras portátiles deberían, cuando sea posible, transportarse como equipaje de mano y de forma disimulada;

b) deberían observarse siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra exposiciones a campos electromagnéticos intensos;

c) los controles para el trabajo en el domicilio se deberían determinar mediante una evaluación de los riesgos y aplicarse los controles convenientes según sea apropiado, por ejemplo, gabinetes para archivos con cerradura, una política de escritorios limpios, controles de acceso a las computadoras y comunicaciones seguras con la oficina (véase también ISO/IEC 18028 *Network Security*);

d) deberían cubrirse con un seguro adecuado los equipos fuera de su lugar de trabajo.

Los riesgos de seguridad, por ejemplo, de daño, robo y escucha, pueden variar mucho según la ubicación y esto debería tenerse en cuenta al determinar los controles más apropiados.

Información adicional

El equipamiento de almacenamiento y procesamiento de la información comprende todo tipo de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes, documentos u otros, que se lleven al domicilio o fuera del lugar habitual de trabajo.

Puede encontrarse en el apartado 11.7.1 más información sobre otros aspectos de la protección de equipos móviles.

9.2.6 Seguridad en la reutilización o eliminación de equipos

Control

Todo aquel equipamiento que contenga medios de almacenamiento debería revisarse para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su disposición.

Guía de implementación

Los dispositivos de almacenamiento con información sensible deberían destruirse físicamente o la información debería destruirse, suprimirse o sobrescribirse usando técnicas para hacer la información original no recuperable, en lugar de utilizar las funciones de borrado o formateado estándar.

Información adicional

Los dispositivos de almacenamiento dañados que contengan datos sensibles pueden requerir una evaluación de riesgo para determinar si estos deberían destruirse físicamente, antes que ser enviados para su reparación o desecho.

La información puede verse comprometida si la reutilización o eliminación de los equipos se realiza de manera descuidada (véase también el apartado 10.7.2).

9.2.7 Retiro de bienes

Control

El equipamiento, la información o el software no deberían retirarse del local de la organización sin previa autorización.

Guía de implementación

Deberían considerarse las siguientes recomendaciones:

a) el equipamiento, la información o el software no deberían retirarse del local de la organización sin previa autorización;

b) deberían identificarse claramente aquellos empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir el retiro de activos fuera de los locales de la organización;

c) debería fijarse un límite de tiempo para el equipamiento retirado y verificar el cumplimiento del retorno;

d) cuando sea necesario y procedente, debería registrarse tanto la salida del equipamiento del local, como el retorno del mismo.

Información adicional

Las instancias de inspección, emprendidas para detectar el retiro de bienes no autorizados, se pueden también realizar para detectar y prevenir el ingreso no autorizado a las instalaciones, de dispositivos de grabación, armas, etc. Tales instancias de inspección deberían realizarse de acuerdo con la legislación y las regulaciones relevantes. Los individuos deberían estar en conocimiento de que estas instancias de inspección serán llevadas a cabo, y las mismas deberían realizarse solamente con la autorización apropiada según los requisitos legales y reguladores.

10 Gestión de comunicaciones y operaciones

10.1 Procedimientos operacionales y responsabilidades

OBJETIVO: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

10.1.1 Procedimientos documentados de operación

Control

Los procedimientos de operación deberían documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.

Guía de implementación

Deberían elaborarse procedimientos documentados para las actividades del sistema asociadas con las instalaciones de comunicaciones y de procesamiento de información, tales como procedimientos de arranque y apagado del computador, respaldo, mantenimiento de equipos, manejo de medios, sala de cómputos, utilización de correo, y seguridad.

Dichos procedimientos deberían especificar las instrucciones necesarias para la ejecución detallada de cada tarea, incluyendo:

a) procesamiento y utilización de la información;

b) respaldo (véase el apartado 10.5);

c) requisitos programables, incluyendo interdependencias con otros sistemas, tiempos de comienzo y finalización de tareas;

d) instrucciones para el manejo de errores u otras condiciones excepcionales, que pudieran presentarse durante la ejecución de la tarea, incluyendo restricciones en el uso de las utilidades de sistema (véase el apartado 11.5.4);

e) soporte en caso de inesperadas dificultades operacionales o técnicas;

f) instrucciones para salida de información y manejo de medios, tales como la utilización de papelería especial o la gestión de salidas confidenciales incluyendo los procedimientos para la disposición segura de la salida de trabajos fallidos (véase los apartados 10.7.2 y 10.7.3);

g) procedimientos de reinicio y recuperación del sistema en caso de falla;

h) la gestión de las pistas de auditoría y de la información del registro del sistema (véase el apartado 10.10).

Los procedimientos de operación, y los procedimientos documentados para las actividades del sistema, deberían tratarse como documentos formales y los cambios autorizados por la dirección. Cuando sea técnicamente posible, los sistemas de información deberían gestionarse de forma consistente, usando los mismos procedimientos, herramientas, y utilidades.

10.1.2 Gestión de cambios

Control

Deberían controlarse los cambios en los sistemas e instalaciones de procesamiento de información.
Guía de implementación

Los sistemas operacionales y el software en producción deberían ajustarse a un estricto control de gestión de cambios.

En particular debería considerarse:

a) identificación y registro de cambios significativos;

b) planificación y pruebas de los cambios;

c) evaluación de los impactos potenciales de tales cambios, incluyendo los impactos en la seguridad;

d) procedimiento formal de aprobación para los cambios propuestos;

e) comunicación de los detalles del cambio a todas las personas involucradas en los mismos;

f) procedimientos de vuelta atrás (*fallback*), incluyendo procedimientos y responsabilidades para abortar y recuperar los cambios sin éxito y de acontecimientos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para asegurar el control satisfactorio de todos los cambios al equipamiento, software o procedimientos. Cuando se realizan los cambios, debería conservarse un registro de auditoría conteniendo toda la información relevante.

Información adicional

El control inadecuado de cambios en las instalaciones y los sistemas de procesamiento de la información es una causa común de las fallas del sistema o de la seguridad. Cambios al ambiente operacional, especialmente al transferir un sistema en desarrollo al estado operacional, pueden afectar la confiabilidad de las aplicaciones (véase también el apartado 12.5.1).

Los cambios a los sistemas operacionales deberían realizarse solamente cuando existe una razón válida para el negocio, por ejemplo un aumento en el riesgo al sistema. La actualización de los sistemas con las últimas versiones del sistema operativo o de la aplicación no siempre favorece el interés del negocio, pues podría introducir más vulnerabilidades e inestabilidad que la versión vigente. Puede también haber una necesidad de capacitación adicional, costos de licencia, soporte, gastos indirectos de mantenimiento y de administración, y hardware nuevo, especialmente durante la migración.

10.1.3 Segregación de tareas

Control

Deberían segregarse las tareas y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

Guía de implementación

La segregación de tareas es un método para reducir el riesgo del uso erróneo accidental o deliberado del sistema. Debería verificarse que ninguna persona pueda tener acceso, modificar o utilizar activos sin autorización o detección. La iniciación de un evento debería separarse de su autorización. La posibilidad de fraude debería considerarse al diseñar los controles.

Las organizaciones pequeñas pueden considerar que este método de control es difícil de lograr, pero el principio debería aplicarse en la medida en que sea posible y practicable. Cuando la segregación sea difícil, deberían considerarse otros controles como la supervisión de las actividades, las pistas de auditoría y la supervisión de la gestión. Es importante que la auditoría de seguridad permanezca independiente.

10.1.4 Separación de los recursos para desarrollo, prueba y producción.

Control

Los recursos para desarrollo, prueba y producción deberían separarse para reducir los riesgos de acceso no autorizado o los cambios al sistema operacional.

Guía de implementación

Debería identificarse el grado de separación entre los ambientes de desarrollo, prueba y producción que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Los siguientes puntos deberían ser considerados:

a) deberían definirse y documentarse las reglas para transferir el software del ambiente de desarrollo al de producción;

b) el software de desarrollo y el de producción deberían, si es posible, funcionar en sistemas y procesadores diferentes, y en dominios o directorios distintos;

c) Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían accederse desde los sistemas en producción, cuando no sea necesario;

d) el ambiente del sistema de prueba debería emular el ambiente del sistema operacional tan real como sea posible;

e) los usuarios deberían emplear perfiles de usuario diferentes para los sistemas en producción y prueba, y los menús deberían exhibir los mensajes de identificación apropiados para reducir el riesgo a errores;

f) los datos sensibles no deberían utilizarse en el ambiente del sistema de prueba (véase el apartado 12.4.2).

Información adicional

Las actividades de desarrollo y prueba pueden causar serios problemas, por ejemplo modificación indeseada de archivos o del ambiente del sistema, o fallo del sistema. En este caso, hay una necesidad de mantener un ambiente estable en el cual realizar la prueba significativa y prevenir el inadecuado acceso del desarrollador.

Si el personal de desarrollo y de prueba tiene acceso al sistema operacional y a su información, puede introducir código no autorizado y no comprobado o alterar datos operacionales. En algunos sistemas esta

capacidad podría ser mal utilizada para realizar fraude, o introducir código no comprobado o malicioso, que puede causar problemas operacionales serios.

Quienes desarrollan y realizan las pruebas imponen una amenaza a la confidencialidad de la información operativa. Las actividades de desarrollo y de prueba pueden causar cambios involuntarios al software o a la información si comparten el mismo ambiente. Por lo tanto, es conveniente separar los recursos para desarrollo, prueba y producción para reducir el riesgo de cambio accidental o acceso no autorizado al software operacional o los datos del negocio (véase el apartado 12.4.2 para la protección de los datos de prueba).

10.2 Gestión de la entrega del servicio por terceras partes

OBJETIVO: Implementar y mantener un nivel apropiado de la seguridad de la información y la entrega del servicio, acorde con los acuerdos de entrega del servicio por terceras partes.

La organización debería verificar la implementación de acuerdos, supervisar el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios entregados cumplen los requisitos acordados con la tercera parte.

10.2.1 Entrega del servicio

Control

Debería asegurarse que los controles de seguridad, las definiciones del servicio y los niveles de entrega incluidos en el acuerdo de entrega del servicio por terceras partes son implementados, operados, y mantenidos por las terceras partes.

Guía de implementación

La entrega del servicio por una tercera parte debería incluir los acuerdos de seguridad, las definiciones del servicio, y los aspectos de la gestión del servicio convenidos. En caso de acuerdos de contratación externa, la organización debería planificar las transiciones necesarias (de información, instalaciones de procesamiento de la información, y cualquier cosa que necesite ser desplazada) y debería garantizar el mantenimiento de la seguridad durante el período de transición.

La organización debería asegurarse que la tercera parte conserva una capacidad de servicio suficiente acorde con los planes realizables, diseñados para asegurarse que los niveles convenidos de la continuidad del servicio están mantenidos ante fallas del servicio o de desastre (véase el apartado 14.1).

10.2.2 Supervisión y revisión de los servicios por terceras partes

Control

Deberían supervisarse y revisarse regularmente los servicios, informes y registros proporcionados por las terceras partes, y deberían realizarse regularmente auditorías.

Guía de implementación

El seguimiento y la revisión de los servicios por terceras partes deberían asegurar el cumplimiento de los términos y condiciones de seguridad de la información de los acuerdos, y que los incidentes y los problemas de la seguridad de la información estén manejados correctamente. Esto debería implicar una relación y un proceso de gestión del servicio entre la organización y la tercera parte para:

a) supervisar niveles de desempeño del servicio para comprobar adherencia a los acuerdos;

b) revisar los informes del servicio producidos por las terceras partes y realizar reuniones de evaluación según los requisitos de los acuerdos;

c) entregar información sobre incidentes de la seguridad de la información y revisión de esta información por las terceras partes y la organización según los requisitos de los acuerdos y las pautas y procedimientos de soporte;

d) revisar pistas de auditoría confeccionadas por las terceras partes y registros de los incidentes de seguridad, de los problemas operacionales, de las fallas, y de interrupciones relacionadas con el servicio entregado;

e) resolver y gestionar cualquier problema identificado.

La responsabilidad de gestionar la relación con terceras partes debería asignarse a un individuo o a un equipo designado de gestión del servicio. Además, la organización debería asegurarse de que las terceras partes asignen responsabilidades de verificación para evaluar la conformidad y hacer cumplir los requisitos de los acuerdos. Los recursos técnicos deberían estar disponibles para supervisar que los requisitos del acuerdo (véase el apartado 6.2.3), en particular los requisitos de seguridad de la información, se estén cumpliendo. Se deberían tomar las acciones adecuadas cuando se observen deficiencias en el servicio de las terceras partes.

La organización debería mantener suficiente control y supervisión en todos los aspectos de la seguridad de la información sensible o crítica, o de las instalaciones de procesamiento de la información accedidas, procesadas o gestionadas por terceras partes. La organización debería asegurar el control sobre actividades de la seguridad tales como gestión del cambio, identificación de las vulnerabilidades, y reportes de incidentes y respuestas de la seguridad de la información mediante una estructura, formato y proceso claramente definido.

Información adicional

En caso de contratación externa, es necesario que la organización sepa que la máxima responsabilidad por la información procesada por una parte contratada externamente sigue siendo de la organización.

10.2.3 Gestión de cambios en los servicios de terceras partes

Control

Los cambios a la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de la seguridad de la información, procedimientos y controles, deberían gestionarse tomando en cuenta la importancia de los sistemas y procesos de negocio que impliquen una nueva valoración de riesgos.

Guía de implementación

El proceso de gestión de cambios a un servicio de terceras partes necesita tomar en cuenta:

a) cambios realizados por la organización para implementar:

1) mejoras a los servicios actuales ofrecidos;
2) desarrollo de nuevos sistemas y aplicaciones;
3) modificaciones o actualizaciones de las políticas y de los procedimientos de la organización;
4) nuevos controles para resolver incidentes de la seguridad de la información y para mejorar la seguridad;

b) cambios en servicios de las terceras partes para implementar:

1) cambios y mejoras en las redes;
2) uso de nuevas tecnologías;
3) adopción de nuevos productos o versiones;
4) nuevas herramientas y ambientes de desarrollo;
5) cambios a la localización física de las instalaciones del servicio;
6) cambio de vendedores.

10.3 Planificación y aceptación del sistema

OBJETIVO: Minimizar el riesgo de fallos de los sistemas. Se requiere una planificación y preparación avanzada para asegurar la disponibilidad de capacidad y recursos adecuados para el desempeño requerido del sistema. Deberían realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema. Deberían establecerse, documentarse y probarse los requisitos operativos de nuevos sistemas antes de su aprobación y utilización.

10.3.1 Gestión de la capacidad

Control

Debería supervisarse y adaptarse el uso de recursos, así como proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.

Guía de implementación

Para cada actividad nueva y en curso, deberían identificarse los requisitos de capacidad. Debería supervisarse y adaptarse el sistema para asegurar, y cuando sea necesario, mejorar la disponibilidad y la eficacia de los sistemas. Deberían ejecutarse controles exhaustivos para indicar problemas a su debido tiempo. Las proyecciones de los requisitos de capacidad futura deberían tomar en cuenta los nuevos requisitos del negocio y del sistema, así como tendencias actuales y proyectadas en la capacidad de procesamiento de la información de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto, los responsables deberían supervisar la utilización de los recursos clave del sistema. Deberían identificar tendencias en uso, particularmente en lo referente a las aplicaciones del negocio o herramientas de administración de sistemas de información.

Los responsables deberían utilizar esta información para identificar y evitar posibles embotellamientos, así como dependencia de personal clave que pudiera presentar una amenaza a la seguridad o a los servicios del sistema, y planificar la acción apropiada.

10.3.2 Aceptación del sistema

Control

Deberían establecerse criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo las pruebas adecuadas del sistema durante el desarrollo y antes de la aceptación.

Guía de implementación

Los directores deberían asegurarse que los requisitos y criterios de aceptación de los nuevos sistemas estén claramente definidos, acordados, documentados y probados. Los nuevos sistemas de información, actualizaciones y nuevas versiones deberían migrarse a producción luego de obtenerse una aceptación formal. Deberían considerarse los siguientes elementos antes de la aceptación formal:

a) requisitos de rendimiento y capacidad de las computadoras;

b) procedimientos de recuperación de errores y reinicio, y planes de contingencia;

c) preparación y prueba de procedimientos operativos de rutina según las normas definidas;

d) conjunto acordado de controles y medidas de seguridad instalados;

e) procedimientos manuales efectivos;

f) disposiciones de continuidad del negocio. (véase el apartado 14.1);

g) evidencia de que la instalación del nuevo sistema no producirá repercusiones negativas sobre los existentes, particularmente en los períodos picos de proceso como a fin de mes;

h) evidencia de que se ha tenido en cuenta el efecto que tendrá el nuevo sistema en la seguridad global de la organización;

i) formación en la operación o utilización de los sistemas nuevos;

j) facilidad de empleo, y cómo esto afecta el funcionamiento del usuario y evita el error humano.

Para nuevos desarrollos importantes, se debería consultar al responsable de operaciones y a los usuarios en todas las etapas del proceso de desarrollo para asegurar la eficacia operacional del diseño del sistema propuesto. Deberían realizarse pruebas apropiadas para confirmar que se han satisfecho completamente todos los criterios de aceptación.

Información adicional

La aceptación puede incluir un proceso formal de certificación y acreditación para verificar que los requisitos de la seguridad se han tratado correctamente.

10.4 Protección contra código malicioso y código móvil

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

Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y código móvil no autorizado.

El software y las instalaciones de procesamiento de información son vulnerables a la introducción de código malicioso como virus informáticos, gusanos de la red, caballos de Troya y bombas lógicas. Los usuarios deberían conocer los peligros que pueden ocasionar el código malicioso y el código móvil no autorizado. Los responsables deberían, cuando sea apropiado, introducir controles para prevenir, detectar y remover el código malicioso y controlar el código móvil.

10.4.1 Controles contra código malicioso

Control

Deberían implantarse controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto a procedimientos adecuados para concientizar a los usuarios.

Guía de implementación

La protección contra el código malicioso debería basarse en el empleo de sistemas de detección y reparación, en la conciencia de la seguridad, y en apropiados controles de acceso al sistema y gestión de cambios. Las siguientes directrices deberían considerarse:

a) establecimiento de una política formal que establezca la prohibición del uso de software no autorizado (véase el apartado 15.1.2);

b) establecimiento de una política formal de protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indicando las medidas protectoras a adoptar;

c) revisiones regulares del contenido de datos y software que soportan los procesos del negocio; la presencia de archivos no aprobados o arreglos no autorizados debería investigarse formalmente;

d) la instalación y actualización regular de antivirus para detección y reparación de software que exploren las computadoras y los soportes de forma rutinaria o como un control preventivo; las verificaciones deberían incluir:

1) comprobación de archivos en medios electrónicos u ópticos, y archivos recibidos a través de redes, para verificar la existencia de código malicioso, antes de su uso;
2) la comprobación para buscar software malicioso, antes de usarlo, de todo archivo adjunto a un correo electrónico o de toda descarga. Esta comprobación que se hará en distintos lugares, por ejemplo, en los servidores de correo, en las computadoras terminales o a la entrada en la red de la organización;
3) comprobación de páginas Web para saber si hay código malicioso;

e) definición de procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación para su uso, la información de los ataques de los virus y la recuperación de éstos (véase los apartados 13.1 y 13.2);

f) preparación de planes de continuidad del negocio apropiados para la recuperación ante los ataques de código malicioso, incluyendo todos los datos y software necesarios de respaldo y las disposiciones para la recuperación (véase la cláusula 14);

g) implementación de procedimientos para recoger regularmente la información, tal como suscripción a las listas de correo y/o comprobación de los sitios Web que brindan la información sobre nuevo código malicioso;

h) implementación de procedimientos para verificar toda la información relativa al software malicioso y asegurarse que los boletines de alerta son precisos e informativos. Los responsables deberían asegurarse que se diferencian los códigos maliciosos reales de los falsos avisos de código malicioso, usando fuentes calificadas, por ejemplo, revistas expertas, sitios de Internet fiables o proveedores de software contra código malicioso. Debería advertirse al personal sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

Información adicional

El uso de dos o más productos de software que protegen contra código malicioso a través del tratamiento de la información de diversos vendedores puede mejorar la eficacia de la protección contra el código malicioso.

El software a proteger contra código malicioso se puede instalar para obtener actualizaciones automáticas de los archivos y los motores de búsqueda para asegurar la actualización de la protección. Además, este software se puede instalar en cada escritorio para realizar verificaciones automáticas.

Debería tenerse especial cuidado para protegerse contra la introducción de código malicioso durante los procedimientos de mantenimiento y de emergencia, evitando que códigos maliciosos puedan saltear los controles.

10.4.2 Controles contra código móvil

Control

Donde el uso de código móvil está autorizado, la configuración debería asegurar que el código móvil autorizado opera de acuerdo con una política de seguridad definida, y debería evitarse la ejecución de código móvil no autorizado.

Guía de implementación

Las siguientes acciones deberían considerarse para protegerse contra las acciones del código móvil no autorizado:

a) ejecución de código móvil en un entorno lógicamente aislado;

b) bloqueo de cualquier utilización de código móvil;

c) bloqueo de recepción de código móvil;

d) activación de medidas técnicas disponibles en sistemas específicos para asegurar el control del código móvil;

e) control de recursos disponibles sobre el acceso del código móvil;

f) controles criptográficos para autenticar el código móvil.

Información adicional

El código móvil es un software que se transfiere de un computador a otro y se ejecuta automáticamente y desarrolla una función específica con poca o nula intervención del usuario. El código móvil está asociado con un número de servicios de software intermedio (*middleware*).

Además, para asegurar que el código móvil no contiene otro código malicioso, el control del código móvil es esencial para evitar su uso no autorizado o la interrupción del sistema, red o recursos de la aplicación y otras brechas de la seguridad de la información.

10.5 Respaldo

OBJETIVO: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de la información. Deberían establecerse procedimientos de rutina para implementar una política y estrategia acordada de respaldo (véase el apartado 14.1) haciendo copias de respaldo de datos y ensayando sus tiempos de restauración.

10.5.1 Respaldo de la información

Control

Deberían hacerse regularmente copias de seguridad de la información y del software y probarse regularmente acorde con la política de respaldo.

Guía de implementación

Deberían mantenerse adecuados soportes de respaldo para asegurar que toda la información esencial y el software puedan recuperarse tras un desastre o fallo de los soportes. Deberían considerarse los siguientes elementos para el respaldo de la información:

a) debería definirse el nivel necesario de información de respaldo;

b) deberían realizarse copias de seguridad de la información seguras y completas, y producirse documentos de restauración;

c) el grado (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio, los requisitos de la seguridad de la información implicada, y la importancia de la información que permita la operación continua de la organización;

d) los respaldos deberían almacenarse en lugar apartado, a una suficiente distancia para la salvaguarda de cualquier daño o desastre en el sitio principal;

e) la información de respaldo debería tener un nivel apropiado de protección ambiental y físico (véase la cláusula 9) consistente con las normas aplicadas en el sitio principal; los controles aplicados a los soportes en el sitio principal se deben ampliar para cubrir el sitio de respaldo;

f) los soportes de respaldo deberían probarse regularmente para asegurarse que pueden ser confiables para el uso cuando sean necesarios;

g) los procedimientos de restauración deberían comprobarse regularmente para asegurar que son eficaces y que pueden ser utilizados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;

h) en situaciones donde la confidencialidad es de importancia, los respaldos deberían protegerse por medio del cifrado.

Las disposiciones de respaldo para los sistemas individuales deberían verificarse regularmente para asegurar que resuelven los requisitos de los planes para la continuidad del negocio (véase la cláusula 14). Para los sistemas críticos, las disposiciones de respaldo deberían cubrir toda la información, usos, y datos de los sistemas necesarios para recuperar el sistema completo en caso de un desastre.

Debería determinarse el período de validez para la información esencial de la organización, y también cualquier requisito para las copias de archivo. (véase el apartado 15.1.3).

Información adicional

Las disposiciones de respaldo se pueden automatizar para facilitar el respaldo y los procesos de restauración. Tales soluciones automatizadas deberían probarse suficientemente antes de la puesta en práctica y en intervalos regulares.

10.6 Gestión de la seguridad de red

OBJETIVO: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, requiere la consideración cuidadosa del flujo de datos, las implicaciones legales, el seguimiento y la protección.

También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por las redes públicas.

10.6.1 Controles de red

Control

Las redes deberían gestionarse y controlarse adecuadamente, para protegerlas contra amenazas, y mantener la seguridad de los sistemas, incluyendo la información en tránsito.

Guía de implementación

Los administradores de redes deberían implantar los controles y medidas requeridas para conservar la seguridad de los datos en las redes de computadoras, así como la protección contra servicios conectados no autorizados. En particular, deberían considerarse los siguientes elementos:

a) La responsabilidad operativa por las redes debería separarse de las operaciones del computador, según sea apropiado (véase el apartado 10.1.3);

b) deberían establecerse responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de usuarios;

c) deberían establecerse, controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que circulen a través de redes públicas, así como para proteger los sistemas conectados (véase los apartados 11.4 y 12.3); también deberían requerirse controles y medidas especiales para mantener la disponibilidad de los servicios de las redes y de las computadoras conectadas;

d) debería utilizarse el registro y la supervisión apropiada para permitir el registro de las acciones relevantes para la seguridad;

e) deberían coordinarse estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información.

10.6.2 Seguridad de los servicios de red

Control

Las características de la seguridad, los niveles del servicio, y los requisitos de la gestión de todos los servicios de red se deberían identificar e incluir en cualquier acuerdo de servicios de red.

Guía de implementación

La capacidad del proveedor de servicio de red para gestionar los servicios acordados de una manera segura deberían ser establecidos y supervisados regularmente, y debería acordarse el derecho a auditar.

Deberían identificarse los acuerdos de seguridad necesarios para servicios particulares, tales como características de la seguridad, niveles de servicio, y requisitos de gestión. La organización debería asegurarse que los proveedores de servicios de red implementen estas medidas.

Información adicional

Los servicios de red incluyen la provisión de conexiones, los servicios de red privados, y las redes con valor agregado, así como soluciones de seguridad para la red tales como cortafuegos (*firewalls*) y sistemas de detección de intrusos.

Las características de la seguridad de los servicios de red podían ser:

a) la tecnología aplicada para los servicios de seguridad de red, tales como autenticación, cifrado, y controles de la conexión de red;

b) parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de la seguridad y de la conexión de red;

c) procedimientos para la utilización del servicio de red para restringir el acceso a los servicios o a los usos de red, cuando sea necesario.

10.7 Manejo de los medios

OBJETIVO: Evitar divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio. Los medios deberían controlarse y protegerse físicamente. Deberían establecerse los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra daño, borrado y acceso no autorizado.

10.7.1 Gestión de los medios removibles

Control

Debería haber implementados procedimientos para la gestión de los medios removibles.

Guía de implementación

Deberían considerarse los siguientes controles:

a) deberían borrarse en forma irrecuperable, cuando no se necesiten más, los contenidos previos de todo medio reutilizable del que se desprenda la organización;

b) cuando sea necesario y práctico, debería requerirse autorización para liberar medios de la organización y deberían registrarse las remociones para mantener la pista de auditoría;

c) todos los medios deberían almacenarse a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes;

d) la información almacenada en medios que necesite estar disponible mayor tiempo que la vida útil del medio (de acuerdo con las especificaciones del fabricante) debería también almacenarse en otra parte para evitar la pérdida de la información debido al deterioro del medio;

e) debería considerarse el registro de los medios removibles para minimizar la oportunidad de pérdida de datos;

f) las unidades de medios removibles sólo deberían habilitarse si existen razones del negocio para hacerlo.

Deberían documentarse claramente todos los procedimientos y niveles de autorización.

Información adicional

Los medios removibles incluyen cintas, discos, discos removibles (*flash disks*), CDs, DVDs y medios impresos.

10.7.2 Eliminación de los medios

Control

Deberían eliminarse los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.

Guía de implementación

Los procedimientos formales de eliminación segura de los medios deberían minimizar el riesgo que personas no autorizadas accedan a información sensible. Deberían considerarse los siguientes elementos:

a) los medios que contengan información sensible deberían almacenarse y eliminarse de forma segura, por ejemplo, incinerándolos o triturándolos, o borrando sus datos para evitar el uso en otra aplicación dentro de la organización;

b) los procedimientos deberían estar disponibles para identificar los controles que requieren la remoción segura;

c) puede ser más fácil que todos los medios sean recogidos y removidos con seguridad, que intentar separar los elementos sensibles;

d) muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios; debería tenerse especial cuidado en seleccionar un contratista conveniente con controles y experiencia adecuados;

e) la disposición de artículos sensibles debería registrarse en lo posible para mantener una pista de auditoría.

Información adicional

La información sensible podría divulgarse con la disposición inadecuada de medios (véase también el apartado 9.2.6 para información sobre la eliminación del equipamiento).

10.7.3 Procedimientos para el manejo de la información

Control

Deberían establecerse procedimientos de utilización y almacenamiento de la información para protegerla de su mal uso o divulgación no autorizada.

Guía de implementación

Deberían elaborarse procedimientos de manejo, procesamiento, almacenamiento y comunicación de la información, de acuerdo con su clasificación (véase el apartado 7.2). Los siguientes elementos deberían considerarse:

a) manejo y etiquetado de todos los medios según su nivel de clasificación indicado;

b) restricciones de acceso para evitar el acceso de personal no autorizado;

c) mantenimiento de un registro formal de los receptores autorizados de datos;

d) asegurar que los datos de entrada estén completos, que el procesamiento se completa adecuadamente y que se valide su salida;

e) protección de los datos que están en cola para su salida en un nivel coherente con su sensibilidad;

f) almacenamiento de los medios en un entorno acorde con las especificaciones del fabricante;

g) mantener la distribución de los datos al mínimo;

h) rotulado claro de todas las copias de los medios para cuidado de los receptores autorizados;

i) revisión de las listas de distribución y de receptores autorizados a intervalos regulares.

Información adicional

Estos procedimientos se aplican a la información en documentos, sistemas de computación, redes, sistemas de comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicio postal, el uso de facsímiles y cualquier otro elemento sensible, por ejemplo, cheques en blanco, facturas.

10.7.4 Seguridad de la documentación de sistemas

Control

La documentación de sistemas debería protegerse contra el acceso no autorizado.

Guía de implementación

Para asegurar la documentación de sistemas, deberían considerarse los siguientes elementos:

a) la documentación de sistemas debería almacenarse en forma segura.

b) la lista de acceso a la documentación de sistemas debería limitarse al máximo, y ser autorizada por el propietario de la aplicación.

c) la documentación de sistemas mantenida en una red pública, o suministrada vía una red pública, debería protegerse adecuadamente.

Información adicional

La documentación de sistemas puede contener variada información sensible, por ejemplo descripciones de procesos de aplicaciones, procedimientos, estructura de datos, procesos de autorización.

10.8 Intercambio de información

OBJETIVO: Mantener la seguridad de la información y software intercambiado dentro de una organización y con cualquier otra entidad.

El intercambio de información y software entre organizaciones debería estar basado en una política de intercambio formal, llevándose a cabo según los acuerdos de intercambio, y debería cumplir con cualquier legislación relevante (véase cláusula 15).

Deberían establecerse procedimientos y normas para proteger la información y los medios físicos que contengan información en transito.

10.8.1 Políticas y procedimientos de intercambio de información

Control

Deberían implementarse políticas formales de intercambio, procedimientos y controles para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación.

Guía de implementación

Los procedimientos y controles a ser seguidos al utilizar medios de comunicación electrónica para el intercambio de información deberían de considerar los siguientes elementos:

a) procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, desviación, y destrucción;

b) procedimientos para la detección de y protección contra código malicioso que pueda ser transmitido por medio del uso de comunicaciones electrónicas. (véase el apartado 10.4.1);

c) procedimientos para proteger la comunicación de información electrónica sensible que se encuentra en la forma de un adjunto;

d) políticas o directrices delineando el uso aceptable de medios de comunicación electrónica (véase el apartado 7.1.3);

e) procedimientos para el uso de comunicaciones inalámbricas, tomando en consideración los riesgos particulares involucrados;

f) responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo, por medio de la difamación, acoso, engaño, reenvió de cadenas de cartas, compra no autorizada, etc.;

g) uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información (véase el apartado 12.3);

h) directrices de retención y eliminación para toda la correspondencia del negocio, incluyendo mensajes, de acuerdo con la legislación y regulaciones nacionales y locales relevantes.

i) no dejar información sensible o crítica en el equipamiento de impresión, por ejemplo, fotocopiadoras, impresoras, facsímiles, en la medida que estas pueden ser accedidas por personal no autorizado;

j) controles y restricciones asociadas con el reenvío de comunicaciones, por ejemplo, reenvío automático de correo electrónico hacia direcciones de correo externo;

k) recordarle al personal que deberían tomar las precauciones apropiadas, por ejemplo, no revelar información sensible evitando el ser escuchados o interceptados al realizar una llamada telefónica por:

1) personas en los alrededores, en particular al utilizar teléfonos móviles.
2) intercepción del cableado, y otras formas de intercepción por medio del acceso físico al aparato o cableado telefónico, o utilizando dispositivos de búsqueda;
3) personas en el extremo del receptor.

l) no dejar mensajes conteniendo información sensible en máquinas contestadoras en la medida que pueden ser escuchadas por personas no autorizadas, almacenadas incorrectamente como resultado de un error de discado;

m) recordarle al personal sobre los problemas de utilizar máquinas de facsímil, llámese:

1) acceso no autorizado al almacenamiento de mensajes para retirarlos.
2) programación deliberada o accidental de las máquinas para enviar mensajes a números específicos.
3) enviar documentos o mensajes a números incorrectos, ya sea por discar incorrectamente o utilizar un número almacenado incorrecto;

n) recordarle al personal el no registrar información demográfica en cualquier software, como la dirección de correo u otra información personal, para evitar su recopilación para usos no autorizados;

o) recordarle al personal que los equipos de facsímil y fotocopiados actuales cuentan con memorias para almacenar páginas en el caso de fallas de papel o transmisión, que serán impresas una vez sea solucionada la falla.

A su vez, al personal debería serle recordado que no deberían tener conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión que no cuenten con paredes a prueba de sonido.

Los medios de intercambio de información deberían de cumplir con todos los requisitos legales relevantes (véase la cláusula 15).

Información adicional

El intercambio de información puede ocurrir por medio del uso de diferentes tipos de medios de comunicación, incluyendo, correo electrónico, voz, facsímil, y video.

El intercambio de software puede ocurrir por medio de diferentes medios, incluyendo descargas desde Internet y adquiriéndolo de proveedores de productos.

Deberían considerarse las implicaciones de negocios, legales y de seguridad asociadas con el intercambio de datos electrónico, comercio electrónico y comunicaciones electrónicas, y los requisitos de controles.

La información puede verse comprometida debido a la falta de concientización, políticas o procedimientos en el uso de medios de intercambio de información, por ejemplo, ser escuchado en un teléfono móvil en un área publica, direccionamiento erróneo de un mensaje de correo electrónico, escucha de máquinas contestadoras, acceso no autorizado a sistemas de mensajes de voz o accidentalmente enviar facsímiles a un equipo equivocado.

Las operaciones del negocio pueden ser perturbadas y la información puede verse comprometida si los medios de comunicación fallan, son interrumpidas o sobrecargadas (véase el apartado 10.3 y la cláusula 14). La información puede verse comprometida si es accedida por usuarios no autorizados (véase la cláusula 11).

10.8.2 Acuerdos de intercambio

Control

Se deberían establecer acuerdos para el intercambio de información y software entre la organización y terceras partas.

Guía de implementación

Los acuerdos de intercambio deberían considerar las siguientes condiciones de seguridad:

a) responsabilidades de gestión para controlar y notificar la transmisión, el envio y recepción;

b) procedimientos para notificar el origen de la transmisión, su envio y recepción;

c) procedimientos para asegurar la trazabilidad y el no repudio;

d) normas técnicas mínimas para el empaquetado y transmisión;

e) acuerdos de custodia (*escrow*);

f) normas para identificar los servicios de mensajería;

g) responsabilidades en el caso de incidentes de seguridad, tales como pérdida de datos;

h) uso de un sistema de etiquetado acordado para la información sensible y crítica, asegurar que el significado de las etiquetas es inmediatamente comprendido y que la información es apropiadamente protegida;

i) propiedad y responsabilidad por la protección de datos, derechos de copia, cumplimiento con licencias de software y consideraciones similares (véase los apartados 15.1.2 y 15.1.4);

j) normas técnicas para la grabación y lectura de información y software;

k) cualquier control especial que puede ser requerido para proteger elementos sensibles, tales como claves criptográficas (véase el apartado 12.3).

Deberían establecerse y mantenerse políticas, procedimientos, y normas para proteger la información y los medios físicos en transito (véase el apartado 10.8.3), y deberían ser referenciados en los acuerdos de intercambio.

El contenido sobre seguridad de cualquier acuerdo debería reflejar la sensibilidad de la información del negocio involucrada.

Información adicional

Los acuerdos pueden ser electrónicos o manuales, y pueden tomar la forma de un contrato formal o condiciones de empleo. Para la información sensible, los mecanismos específicos utilizados para el intercambio de dicha información deberían ser consistentes para todas las organizaciones y tipos de acuerdos.

10.8.3 Medio físico en tránsito

Control

Los medios conteniendo información deberían ser protegidos contra accesos no autorizados, su mal uso o corrupción durante el transporte fuera de las fronteras físicas de la organización.

Guía de implementación

Deberían considerarse las siguientes directrices para proteger los medios de información durante su transporte entre sitios:

a) deberían ser utilizados transportistas o mensajeros confiables;

b) debería ser acordada una lista de mensajeros autorizados con la dirección;

c) se deberían desarrollar procedimientos para chequear la identificación del mensajero;

d) el empaquetado debería ser suficiente a los efectos de proteger el contenido ante cualquier daño físico que pueda ocurrir durante el transito, de acuerdo con cualquier especificación del fabricante (por ejemplo para el software), por ejemplo, protegiendo contra cualquier factor ambiental que pueda afectar a los medios, tales como exceso de calor, humedad o campos electromagnéticos;

e) donde sea necesario, deberían ser adoptados controles para proteger información sensible de su divulgación o modificación no autorizada; ejemplos:

1) uso de contenedores sellados;
2) entrega en mano;
3) paquetes que evidencian violaciones (que revelan cualquier intento de obtener acceso al contenido);
4) en casos excepcionales, distribuir el envio en más de una entrega y el envió por diferentes rutas.

Información adicional

La información puede ser vulnerable al acceso no autorizado, uso incorrecto o corrupción durante su transporte físico, por ejemplo, al enviar medios por el servicio postal o un mensajero.

10.8.4 Mensajería electrónica

Control

La información contenida en la mensajería electrónica debería ser apropiadamente protegida.

Guía de implementación

Las consideraciones de seguridad para la mensajería electrónica deberían incluir lo siguiente:

a) proteger mensajes del acceso no autorizado, modificación o negación de servicio;

b) asegurar el correcto direccionamiento y transporte de los mensajes;

c) confiabilidad y disponibilidad general del servicio;

d) consideraciones legales, por ejemplo, requisitos para firmas digitales;

e) obtener la aprobación antes de utilizar servicios públicos externos, tales como mensajería instantánea y compartir archivos;

f) fuertes niveles de autenticación controlando el acceso desde redes de acceso público.

Información adicional

La mensajería electrónica, como el correo electrónico, intercambio electrónico de datos (*EDI*), y mensajería instantánea juegue un rol cada vez más importante en las comunicaciones del negocio. La mensajería electrónica tiene diferentes riesgos que las comunicaciones en base a papel.

10.8.5 Sistemas de Información de negocio

Control

Deberían desarrollarse y ponerse en práctica una política de control y procedimientos para proteger la información asociada con la interconexión de sistemas de información de negocio.

Guía de implementación

Las consideraciones de las implicaciones que tiene la interconexión de tales recursos para la seguridad y para el negocio deberían incluir:

a) vulnerabilidades conocidas en los sistemas administrativos y de la contabilidad donde la información es compartida entre partes diferentes de la organización;

b) las vulnerabilidades de información en sistemas de comunicación de negocio, por ejemplo registrando llamadas telefónicas o teleconferencias, confidencialidad de llamadas, almacenaje de facsímiles, abriendo correo, distribución de correo;

c) política y controles apropiados para poder gestionar la información compartida;
d) excluir las categorías de información sensibles del negocio y documentos clasificados si el sistema no provee un nivel apropiado de protección (véase el apartado 7.2);

e) restringir el acceso a información de bitácoras relacionada con individuos seleccionados, por ejemplo, personal que trabaja sobre proyectos sensibles;

f) las categorías de personal, contratistas o socios de negocio permitidos para usar el sistema y las posiciones desde las cuales puede ser teniendo acceso (véase los apartados 6.2 y 6.3);

g) restricción de instalaciones a las categorías específicas de usuario;

h) identificación del estado de usuarios, por ejemplo, los empleados de la organización o contratistas en directorios en beneficio de otros usuarios;

i) la retención y el respaldo sostenido de información del sistema (véase el apartado 10.5.1);

j) requisitos y acuerdos de vuelta atrás (véase la cláusula 14).

Información adicional

Los sistemas de información de oficina permiten diseminar y compartir más rápido información de negocio utilizando una combinación de: documentos, computadoras, informática móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios / prestaciones postales y máquinas de facsímil.

10.9 Servicios de comercio electrónico

OBJETIVO: Asegurar la seguridad de los servicios de comercio electrónico, así como su uso seguro.

Deberían considerarse las implicaciones de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo transacciones en línea (*on-line*), y los requisitos de control. Debería también considerarse la integridad y disponibilidad de información electrónicamente publicada por medio de sistemas públicos.

10.9.1 Comercio electrónico

Control

La información involucrada en el comercio electrónico sobre redes públicas debería ser protegida ante actividades fraudulentas, disputas contractuales, y su divulgación o modificación no autorizada.

Guía de implementación

Las consideraciones de seguridad para el comercio electrónico deberían incluir las siguientes:

a) el nivel de confianza que cada parte requiere en la identidad declarada por los otros, por ejemplo, por medio de autenticación;

b) proceso de autorización asociado con quien puede establecer precios, emitir o firmar documentos de comercio claves;

c) asegurar que los socios de negocios son completamente informados sobre sus autorizaciones;

d) determinar y cumplir los requisitos de confidencialidad, integridad, prueba de envío y recepción de documentos claves, y el no repudio de contratos, por ejemplo, asociados con procesos de ofrecimientos y contratos;

e) el nivel de confianza requerido en la integridad de la lista de precios publicitada;

f) la confidencialidad de cualquier dato o información sensible;

g) la confidencialidad e integridad de cualquier orden de transacción, información de pago, detalles de dirección de envío, y confirmación de recepción;

h) el grado de verificación apropiado para chequear la información de pago brindada por un cliente;

i) seleccionar la mejor forma de acuerdo del pago para protegerse contra fraudes;

j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de la orden;

k) evitar la perdida o duplicación de la información de la transacción;

l) responsabilidades asociadas a cualquier transacción fraudulenta;

m) requisitos de seguros.

Muchas de las consideraciones anteriores pueden ser logradas por medio del uso de controles criptográficos (véase el apartado 12.3), tomando en consideración el cumplimiento de requisitos legales (véase el apartado 15.1, especialmente 15.1.6 por legislación sobre criptografía).

Acuerdos de comercio electrónico entre socios de negocios deberían estar soportados por un acuerdo documentado que comprometa a ambas partes con los términos de comercio acordados, incluyendo detalles de autorización (véase el punto b). Otros acuerdos con servicios de información y proveedores de redes de valor agregado pueden ser necesarios.

Los sistemas de comercio públicos deberían publicar los términos de negocios a sus clientes.

También debería considerarse la resistencia al ataque del servidor central (*host*) utilizado para el comercio electrónico, y las implicaciones de seguridad de cualquier interconexión de redes requerido para la implementación de los servicios de comercio electrónico (véase el apartado 11.4.6).

Información adicional

El comercio electrónico es vulnerable a un número de amenazas de red que pueden resultar en actividad fraudulenta, disputas de contratos, y divulgación o modificación de la información.

El comercio electrónico puede hacer uso de métodos de autenticación seguros, por ejemplo, utilizando criptografía de clave pública y firmas digitales (véase el apartado 12.3) para reducir el riesgo. También pueden ser utilizadas terceras partes de confianza, donde sus servicios sean necesarios.

10.9.2 Transacciones en línea

Control

La información implicada en transacciones en línea debería protegerse para prevenir la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.

Guía de implementación

Las consideraciones de seguridad para transacciones en línea deberían incluir lo siguiente:

a) el empleo de firmas electrónicas por cada una de las partes implicadas en la transacción;

b) todos los aspectos de la transacción, por ejemplo asegurar que:
   1) las cartas credenciales de usuario de todas las partes son válidas y verificadas;
   2) la transacción permanece confidencial; y
   3) la privacidad asociada con todas las partes implicadas es conservada;

c) el canal de comunicación entre todas las partes implicados es cifrada;

d) el protocolo utilizado para comunicarse entre todas las partes implicadas es seguro;

e) el almacenamiento de los detalles de transacción es localizado fuera de cualquier ambiente público accesible, por ejemplo, en una plataforma de almacenamiento que exista en la Intranet de la organización, y no conservado y expuesto en un medio de almacenamiento directamente accesible desde Internet;

f) cuando se emplea una autoridad confiable (por ejemplo, para propósitos de emitir y mantener firmas digitales y / o certificados digitales) la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado / firma.

Información adicional

El grado de los controles adoptados tendría que ser proporcional con el nivel del riesgo asociado con cada tipo de transacción en línea.

Las transacciones pueden tener que cumplir con leyes, reglas, y regulaciones en la jurisdicción en la cual la transacción es generada, procesada, completada, y/o almacenada.

Existen muchos tipos de transacciones que pueden ser realizadas en línea, por ejemplo, contractuales, financieras, etc.

10.9.3 Información accesible públicamente

Control

Debería protegerse la integridad de la información de un sistema accesible públicamente, para prevenir la modificación no autorizada.

Guía de implementación

El software, datos y otra información que requiera un alto nivel de integridad y que estén accesibles públicamente, deberían protegerse por mecanismos adecuados, por ejemplo, firmas digitales (véase el apartado 10.3.3). Los sistemas accesibles públicamente, deberían probarse contra debilidades y fallas antes que la información esté disponible.

Debería haber un proceso de aprobación formal antes de que la información esté accesible públicamente. Además, toda la entrada proveniente del exterior al sistema debería ser verificada y aprobada.

Los sistemas electrónicos de edición, sobre todo aquellos que permiten la retroalimentación y el ingreso directo de información, deberían controlarse con cuidado de modo que:

a) la información se obtenga en cumplimiento con toda la legislación sobre protección de datos (véase el apartado 15.1.4);

b) el ingreso de la información a, y el procesamiento por, el sistema de edición será procesado completamente y con exactitud de manera oportuna;

c) la información sensible será protegida durante la recolección, procesamiento, y almacenamiento;

d) el acceso al sistema de edición no permita el acceso no planeado a redes a las cuales el sistema se conecta.

Información adicional

La información sobre un sistema accesible públicamente, por ejemplo, la información sobre un servidor Web accesible vía la Internet, puede tener que cumplir con leyes, reglas, y regulaciones en la jurisdicción en la cual el sistema es localizado, donde el comercio tiene lugar o donde el propietario(s) reside. La modificación no autorizada de información publicada puede dañar la reputación de la organización.

10.10 Seguimiento

OBJETIVO: Detectar actividades de procesamiento de información no autorizadas.

Deberían supervisarse los sistemas y registrarse los eventos de seguridad de la información. Registros del operador y de fallas deberían ser utilizados para asegurar que los problemas en los sistemas de información son identificados.

La organización debería cumplir con todos los requisitos legales aplicables a sus actividades de seguimiento y registro.

El seguimiento del sistema debería ser utilizado para chequear la eficacia de los controles adoptados y verificar la conformidad a una política de acceso modelo.

10.10.1 Registros de auditoría

Control

La grabación de registros de auditoría de actividades de usuario, excepciones, y eventos de seguridad de la información deberían ser producidos y guardados durante un período acordado para ayudar en futuras investigaciones y en la supervisión del control de acceso.

Guía de implementación

Los registros de auditoría deberían incluir, cuando sea relevante:

a) identificación (*ID*) de usuario;

b) fechas, horas, y los detalles de acontecimientos claves, por ejemplo, inicio y fin de una sesión;

c) identidad de la terminal y ubicación, si es posible;

d) registros de los intentos aceptados y rechazados de acceso al sistema;

e) registros de los intentos aceptados y rechazados de acceso a los datos y otros recursos;

f) cambios a la configuración de sistema g) empleo de privilegios;

h) empleo de utilitarios y aplicaciones de sistema;

i) archivos accedidos y la clase de acceso;

j) direcciones y protocolos de conexiones de una red;

k) alarmas levantadas por el sistema de control de acceso;

l) activación y desactivación de sistemas de protección, como sistemas de antivirus y sistemas de detección de intrusos.

Información adicional

Los registros de auditoría pueden contener datos personales confidenciales e indiscretos. Deberían tomarse medidas de protección de privacidad (véase también el apartado 15.1.4). De ser posible, los administradores de sistema no deberían tener el permiso de borrar o desactivar los registros de sus propias actividades (véase el apartado 10.1.3).

10.10.2 Supervisión del uso de sistemas

Control

Deberían establecerse procedimientos para supervisar el empleo de instalaciones de procesamiento de la información y revisarse con regularidad los resultados de las actividades de supervisión.

Guía de implementación

El nivel de supervisión requerido para instalaciones individuales debería determinarse según una evaluación de riesgo. Una organización debería cumplir con todas los requisitos legales relevantes aplicables a su actividades de supervisión. Las áreas que deberían ser consideradas incluyen:

a) acceso autorizado, incluyendo detalles tales como:

1) la identificación (*ID*) de usuario;
2) la fecha y hora de acontecimientos claves;
3) los tipos de eventos;
4) los archivos accedidos;
5) el programa/utilitario utilizado;

b) todas las operaciones privilegiadas, tales como:

1) empleo de cuentas privilegiadas, por ejemplo, supervisor, *root*, administrador;
2) arranque y apagado del sistema;
3) conexión/desconexión de dispositivos de entrada-salida (*I/O*);

c) intentos de acceso no autorizados, tales como:

1) acciones de usuario fallidas o rechazadas;
2) acciones fallidas o rechazadas que implican datos y otros recursos;
3) violaciones de política de acceso y notificaciones para puertas de enlace (*gateway*) y cortafuegos (*firewall*) de red;
4) alerta de sistemas de detección de intrusión propietarios;

d) alertas o fallas del sistema tales como:

1) alarmas o mensajes de consola;
2) excepciones del registro del sistema;
3) gestión de alarmas de red;
4) alarmas levantadas por el sistema de control de acceso;

e) cambios o intentos de cambiar, configuraciones y controles de seguridad del sistema.

La frecuencia con la cual se revisan los resultados de las actividades de supervisión debería depender de los riesgos involucrados. Los factores de riesgos que deberían considerarse incluyen:

a) criticidad de los procesos de aplicación;

b) valor, sensibilidad, y criticidad de la información implicada;

c) experiencia pasada de infiltración y mal uso del sistema, y la frecuencia de vulnerabilidades explotadas;

d) la extensión de las interconexiones del sistema (en particular con redes públicas);
e) herramientas de registro desactivadas.

Información adicional

Es necesario utilizar procedimientos de supervisión para asegurar que los usuarios sólo realizan las actividades que explícitamente se les han autorizado.

La revisión del registro implica la comprensión de las amenazas enfrentadas por el sistema y la forma en que se pueden originar. En el apartado 13.1.1 se presentan ejemplos de eventos que podrían requerir investigación adicional en caso de incidentes de seguridad de la información.

10.10.3 Protección de la información de registros (logs)

Control

Los medios de registro y la información de registros deberían ser protegidos contra su alteración y acceso no autorizado.

Guía de implementación

Los controles deberían proteger contra cambios no autorizados y problemas operativos en los medios de registro, incluyendo:

a) alteración a los tipos de mensajes que son registrados;

b) archivos de registros (*logs*) siendo editados o eliminados;

c) capacidad de almacenamiento de los medios de archivo de registro excedida, resultando en la falla en el registro de eventos o en la sobre-escritura de eventos pasados.

Alguna auditoría de registros puede ser requerida para ser archivada como parte de la política de retención de registros o debido a requisitos para recolectar y retener evidencia (véase el apartado 13.2.3).

Información adicional

Los registros del sistema a menudo contienen un vasto volumen de información, mucha de la cual no tiene relación con la supervisión de seguridad. Para ayudar a la identificación de eventos significativos para la supervisión de seguridad, debería considerarse el copiado automático de los tipos de mensajes apropiados a un registro secundario, y/o el uso de herramientas del sistema adecuadas o herramientas de auditoría para realizar la interrogación y racionalización de los archivos.

Los registros del sistema necesitan ser protegidos, debido a que si la información puede ser modificada o eliminada, su existencia puede crear una falsa sensación de seguridad.

10.10.4 Registros del administrador y operador

Control

Las actividades del administrador y operador del sistema deberían de ser registradas.

Guía de implementación

Los registros deberían de incluir:

a) la hora en la cual un evento (exitoso o fallido) ocurre;

b) información sobre el evento (por ejemplo, archivos manejados) o falla (por ejemplo, errores ocurridos y acciones correctivas emprendidas);

c) qué cuenta y que administrador u operador fue involucrado;

d) qué procesos fueron involucrados.

Los registros del administrador y operador deberían de ser revisados de forma regular.

Información adicional

Un sistema de detección de intrusión, gestionado fuera del control de los administradores de sistema y de red, puede ser utilizado para supervisar el cumplimiento de actividades de los administradores de sistema y de red.

10.10.5 Registro de fallas.

Control

Las fallas deberían de ser registradas, analizadas y tomadas las acciones apropiadas.

Guía de implementación

Las fallas reportadas por los usuarios o programas relativos a problemas con el procesamiento de información o sistemas de comunicaciones deberían ser registradas. Deberían existir reglas claras para manejar las fallas reportadas, incluyendo:

a) revisión de registros de fallas para asegurar que han sido satisfactoriamente resueltas;

b) revisión de medidas correctivas para asegurar que los controles no se han visto comprometidos, y que la acción emprendida ha sido autorizada.

Se debería asegurar que el registro de errores está habilitado, si esta funcionalidad del sistema se encuentra disponible.

Información adicional

El registro de errores y fallas puede impactar en el desempeño de un sistema. Estos registros deberían de ser establecidos por personal competente, y el nivel de registro requerido para los sistemas individuales debería de ser determinado por un análisis de riesgos, que tenga en cuenta la degradación del sistema.

10.10.6 Sincronización de relojes

Control

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de la organización o dominio de seguridad deberían estar sincronizados con una fuente de horario confiable acordada.

Guía de implementación

Cuando una computadora o dispositivo de comunicaciones tiene la capacidad de operar un reloj de tiempo real, este reloj debería establecerse como el estándar acordado, por ejemplo, el tiempo coordinado universal (*UTC*) o el horario estándar local. Dado que ciertos relojes atrasan con el tiempo, debería existir un procedimiento que chequea y corrija cualquier variación significativa.

La correcta interpretación del formato fecha/hora es importante para asegurar que las marcas de tiempo reflejan la fecha y hora real. Características locales (por ejemplo cambio de horario de verano) deberían de ser tenidas en cuenta.

Información adicional

La configuración correcta de relojes de los ordenadores es importante para asegurar la exactitud de los registros de auditoría, que pueden requerirse para investigaciones o como pruebas en casos legales o disciplinarios. Los registros inexactos de auditoría pueden dificultar tales investigaciones y restar credibilidad a tales pruebas. Un reloj vinculado a una difusión de tiempo de un reloj nacional atómico puede ser usado como el reloj maestro para registrar sistemas. Un protocolo de tiempo de red puede utilizarse para mantener a todos los servidores en sincronización con el reloj maestro.

11 Control de acceso

11.1 Requisitos de negocio para el control de acceso

OBJETIVO: Controlar el acceso a la información.

Los accesos a la información, a las instalaciones de procesamiento de la información y a procesos del negocio deberían ser controlados sobre la base de requisitos de negocio y seguridad.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

11.1.1 Política de Control de Acceso

Control

Debería establecerse, documentarse y revisarse una política de control de acceso, basada en requisitos de negocio y seguridad para el acceso.

Guía de implementación

Las reglas de control de acceso y derechos para cada usuario o grupo de usuarios deberían estar claramente establecidas en una política de control de acceso. Los controles de acceso son tanto lógicos como físicos (véase también la cláusula 9), y éstos deberían considerarse en forma conjunta. Los usuarios y los proveedores de servicio deberían ser provistos de una declaración clara de los requisitos de negocio que deberían cumplir para los controles de acceso.

La política debería tener en cuenta lo siguiente:

a) requisitos de seguridad de aplicaciones de negocio individuales;

b) identificación de toda la información relacionada a las aplicaciones del negocio y los riesgos que la información está enfrentando; c) políticas para autorización y distribución de la información, por ejemplo la necesidad de conocer el principio y los niveles de seguridad y clasificación de la información (véase el apartado 7.2);

d) consistencia entre los controles de acceso y las políticas de clasificación de la información de los diferentes sistemas y redes;

e) legislación relevante y obligaciones contractuales con respecto a la protección de acceso a los datos o servicios (véase el apartado 15.1);

f) perfiles estándar de acceso de usuario para roles comunes en al organización;

g) gestión de derechos de acceso en un ambiente distribuido y de redes que reconozca todos los tipos de conexión posibles;

h) separación de roles de control de acceso, por ejemplo, pedido de acceso, autorización de acceso, administración de acceso;

i) requisitos para autorizaciones formales de pedidos de acceso (véase el apartado 11.2.1);

j) pedidos para revisión periódica de controles de acceso (véase el apartado 11.2.4);

k) remoción de derechos de acceso (véase el apartado 8.3.3)

Información adicional

Debería tenerse cuidado cuando se están especificando las reglas de control de acceso en considerar:

a) diferenciación entre reglas que siempre deben ser acatadas y directrices que son opcionales o condicionales;

b) establecimiento de reglas basadas sobre la premisa “Todo está generalmente prohibido salvo que expresamente sea permitido” mas que sobre la regla mas débil “Todo esta generalmente permitido salvo que sea expresamente prohibido”;

c) cambios en las etiquetas de la información (véase el apartado 7.2) que son iniciados automáticamente por los recursos de procesamiento de información y aquellos que son iniciados a discreción de un usuario;

d) cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por un administrador;

e) reglas, que requieren una aprobación específica antes de habilitarse y aquellas que no lo requieren;

Las reglas de control de acceso deber ser soportadas por procedimientos formales y responsabilidades claramente definidas (véase por ejemplo, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Gestión del acceso de usuarios

OBJETIVO: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.

Deberían existir procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información y a los servicios.

Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso del usuario, desde el registro inicial de nuevos usuarios hasta la cancelación final del registro de usuarios que no requieren más acceso a los sistemas de información y a los servicios. Debería tenerse especial atención, cuando corresponda, a la necesidad de control de la asignación de derechos de acceso privilegiados, que permiten a los usuarios sobrescribir los sistemas de control.

11.2.1 Registro de usuarios

Control

Debería existir un procedimiento formal de registro y cancelación de registro para otorgar y revocar los accesos a todos los servicios y sistemas de información.

Guía de implementación

El procedimiento de control de acceso para el registro y cancelación de registro del usuario debería incluir:

a) utilización de la identificación única de usuario (*IDs*) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso del identificador de grupo, debería permitirse solamente cuando sea necesario por razones de negocio u operativas, y deberían ser aprobadas y documentadas;

b) verificación de que el usuario tenga autorizaron del dueño del sistema para el uso del servicio ó el sistema de información; aprobación separada para los derechos de acceso para la gestión podría ser apropiado;

c) verificación de que el nivel de acceso otorgado sea apropiado para el propósito del negocio (véase el apartado 11.1) y que es consistente con la política de seguridad, por ejemplo que no compromete la segregación de tareas (véase el apartado 10.1.3);

d) entregar al usuario una declaración de sus derechos de acceso;

e) requerir que los usuarios firmen declaraciones indicando que ellos comprenden las condiciones de acceso;

f) asegurar que los proveedores de servicio no provean acceso hasta que los procedimientos de autorización hayan sido completados;

g) mantener un registro formal de todas las personas registradas que usan el servicio;

h) borrar inmediatamente o bloquear los derechos de acceso de los usuarios que hayan cambiado roles o tareas o dejado la organización;

i) periódicamente realizar una verificación para borrar o bloquear las cuentas e identificación de usuarios (*IDs*) redundantes (véase el apartado 11.2.4);

j) asegurar que las identificaciones de usuarios (*IDs*) redundantes no se otorgan a otros usuarios.

Información adicional

Se debería considera el establecimiento de funciones de acceso de usuario basadas en los requisitos del negocio que resuman una variedad de derechos de acceso en perfiles comunes para el acceso de usuario. Las solicitudes y revisiones de acceso (véase el apartado 11.2.4) se gestionan más fácilmente en el ámbito de dichas funciones que en el ámbito de derechos particulares.

Es conveniente considerar la inclusión de cláusulas en los contratos del personal y de los servicios que especifiquen las sanciones si el personal o los agentes del servicio intentan el acceso no autorizado (véase los apartados 6.1.5, 8.1.3 y 8.2.3).

11.2.2 Gestión de privilegios

Control

Debería restringirse y controlarse la asignación y uso de privilegios.
Guía de implementación

Sistemas multiusuario que requieren protección contra accesos no autorizados deberían tener la asignación de privilegios controlada a través de procedimientos formales de autorización. Deberían considerarse los siguientes elementos:

a) los privilegios de acceso asociados con cada producto del sistema, por ejemplo sistema operativo, sistema de gestión de base de datos y de cada aplicación, y debería identificarse a los usuarios a los que es necesario asignar tales privilegios;

b) los privilegios deberían ser asignados a usuarios sobre la base de necesidad de uso y sobre la base de evento por evento, alineados con la política de control de acceso (véase el apartado 11.1.1), es decir, el requisito mínimo para su rol funcional, solo cuando es necesario;

c) deberían ser mantenidos un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que el procedimiento de autorización no sea completado;

d) debería ser promovido el desarrollo y utilización de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios;

e) debería ser promovido el desarrollo y uso de programas que eviten la necesidad de funcionar con privilegios;

f) los privilegios deberían ser asignados a una identificación de usuario (*ID*) diferente de la utilizada para uso normal del negocio.

Información adicional

El uso inapropiado de los privilegios de administración del sistema (cualquier característica o recurso de un sistema de información que habilite al usuario a hacer caso omiso de los controles del sistema o de la aplicación) puede ser un factor importante de contribución a las fallas o brechas de los sistemas.

11.2.3 Gestión de contraseñas del usuario

Control

La asignación de contraseñas debería controlarse a través de un proceso formal de gestión.

Guía de implementación

El proceso debería incluir los siguientes requisitos:

a) se debería exigir a los usuarios que firmen una declaración de para mantener confidencialidad sobre las contraseñas personales y mantener las contraseñas de grupo dentro de los miembros del grupo; esta declaración firmada podría estar incluida dentro de los términos de empleo (véase el apartado 8.1.3);

b) cuando se exige a los usuarios el mantener sus propias contraseñas, ellos deben ser provistos inicialmente con una contraseña segura temporal (véase el apartado 11.3.1), que estén forzados a cambiar inmediatamente;

c) establecer procedimientos para verificar la identidad del usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva;

d) las contraseñas temporales deberían ser dadas a los usuarios de un modo seguro; deberían ser evitados el uso de mensajes de correo electrónico de terceras partes o no protegidos (en texto claro);

e) las contraseñas temporales deberían ser únicas para un individuo y no deberían ser descifrables;

f) los usuarios deberían acusar el recibo de las contraseñas;

g) las contraseñas nunca deberían ser almacenadas en sistemas de computadoras o en forma no protegida;

h) las contraseñas por defecto de los vendedores deberían cambiarse inmediatamente luego de la instalación del software o sistemas.

Información adicional

Las contraseñas son un medio común de verificación de la identidad del usuario antes de que se les otorguen accesos a los sistemas de información o a los servicios de acuerdo a la autorización que tenga el usuario. Si es apropiado, deberían considerarse otras tecnologías disponibles para la identificación y autenticación del usuario, tales como biometría, por ejemplo, verificación de huella digital, verificación de firma, y uso de señales de hardware (*hardware tokens*), por ejemplo tarjetas inteligentes.

11.2.4 Revisión de derechos de acceso de usuario

Control
La dirección debería revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

Guía de implementación

La revisión de los derechos de acceso debería considerar las siguientes recomendaciones:

a) los derechos de acceso de usuarios deberían ser revisados a intervalos regulares, por ejemplo, cada seis meses, y luego de cualquier cambio, tal como una promoción, una degradación, o terminación del empleo (véase el apartado 11.2.1);

b) los derechos de acceso de usuario deberían ser revisados y reasignados cuando se mueve de un empleo a otro dentro de la misma organización;

c) las autorizaciones para derechos de acceso privilegiados (véase el apartado 11.2.2) deberían ser revisados a intervalos mas frecuentes; por ejemplo cada tres meses;

d) debería verificarse la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados;

e) los cambios en las cuentas privilegiadas deberían registrarse para su revisión periódica.

Información adicional

Es necesario revisar los derechos de acceso de usuarios regularmente para mantener un control de acceso efectivo sobre el acceso a los datos y servicios de información.

11.3 Responsabilidades del usuario

OBJETIVO: Prevenir el acceso de usuario no autorizado, y el robo o compromiso de la información y de las instalaciones de procesamiento de la información.

La cooperación de usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben ser enterados de sus responsabilidades para mantener los controles de acceso, particularmente teniendo en cuenta el uso de contraseñas y la seguridad del equipamiento del usuario.

Una política de escritorio y pantallas limpios, debería ser implementada para reducir el riesgo de acceso no autorizado o daño a papeles, medios, e instalaciones de procesamiento de la información.

11.3.1 Uso de Contraseña

Control

Debería exigirse a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de contraseñas.

Guía de implementación

Todos los usuarios deberían ser advertidos en cuanto a:

a) mantener confidencialidad sobre la contraseña;

b) evitar mantener un registro de contraseñas (por ejemplo en papel, archivo de software o dispositivo de mano *"hand-held device"*), salvo que este medio pueda ser almacenado en forma segura y el método de almacenamiento haya sido aprobado;

c) cambiar las contraseñas toda vez que haya una indicación de riesgo en el sistema o en la contraseña;
d) seleccionar contraseñas de calidad con suficiente largo mínimo que sean:

1) fáciles de recordar;
2) no se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo, nombres, números telefónicos, fechas de nacimiento, etc.;
3) no vulnerables a ataques tipo diccionario (es decir, que no consistan en palabras incluidas en diccionarios);
4) libres de caracteres idénticos sucesivos ya sean todos numéricos o alfabéticos;

e) cambiar las contraseñas a intervalos regulares o basados en el número de accesos (las contraseñas de cuentas privilegiadas deberían ser cambiadas más frecuentemente que las contraseñas normales), y evitar la reutilización o reciclaje de claves viejas;

f) cambiar las contraseñas temporales en la primera conexión;

g) no incluir contraseñas en ningún proceso automatizado de conexión, por ejemplo almacenado en una macro o función clave;

h) no compartir las contraseñas de usuario individuales;

i) no utilizar la misma contraseña para propósitos del negocio y particulares;

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que pueden usar una sola contraseña de calidad

(véase el punto d) para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

Información adicional

La gestión del sistema de mesa de ayuda que tiene que ver con la pérdida u olvido de contraseñas necesita especial cuidado pues esta puede ser también un medio de ataque al sistema de contraseñas.

11.3.2 Equipamiento desatendido por el usuario

Control

Los usuarios deberían asegurarse que los equipos desatendidos tienen la protección apropiada.

Guía de implementación

Todos los usuarios deberían ser advertidos de los requisitos y procedimientos de seguridad para proteger equipamiento desatendido, así como de su responsabilidad de implementar tal protección. Se debería advertir a los usuarios sobre:

a) terminar sesiones activas cuando son finalizadas, salvo que se les pueda asegurar por un mecanismo de bloqueo apropiado, por ejemplo un protector de pantalla protegido con contraseña;

b) desconectarse de los computadores centrales, servidores y estaciones de trabajo de oficina cuando la sesión es finalizada (por ejemplo no apagar solo el monitor de la terminal o estación de trabajo);

c) asegurar a las estaciones de trabajo de uso no autorizado mediante una clave de bloqueo o un control equivalente, por ejemplo contraseña de acceso cuando no se encuentra en uso (véase también el apartado 11.3.3).

Información adicional

Equipamiento instalado en áreas usuarias, por ejemplo estaciones de trabajo o servidores de archivo, pueden requerir protección específica frente a acceso no autorizado cuando se deja desatendido por un periodo largo.

11.3.3 Política de escritorio y pantalla limpios.

Control

Se debería adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.

Guía de implementación

Una política de escritorio limpio debería tener en cuenta la clasificación de la información (véase el apartado 7.2), requisitos legales y contractuales (véase el apartado 15.1), y los aspectos culturales y de riesgo de la organización correspondientes. Deberían considerarse las siguientes recomendaciones:

a) cuando no se requiere la información sensible o crítica del negocio, contenida por ejemplo en medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave (idealmente una caja fuerte, un gabinete u otro mueble de seguridad), especialmente cuando la oficina está vacía;

b) las computadoras y terminales deberían ser desconectadas o protegidas con un mecanismo de bloqueo de pantalla y teclado controlado por contraseña, una señal (*token*), o mecanismo de autenticación de usuario

similar cuando está desatendida, y debería ser protegida por claves de bloqueo, o contraseñas u otros controles cuando no esta en uso;

c) deberían ser protegidos puntos de ingreso y egreso de correo electrónico y máquinas de facsímil desatendidas;

d) debería prevenirse el uso no autorizado de fotocopias y otras tecnologías de reproducción (por ejemplo escáneres, cámaras digitales);

e) documentación conteniendo información clasificada o sensible debería retirarse de las impresoras inmediatamente.

Información adicional

Una política de escritorio y pantalla limpios, reduce los riesgos de acceso no autorizado, pérdida o daño a la información durante y fuera de las horas normales de trabajo. Cofres u otras formas de almacenamiento seguro pueden también proteger información almacenada dentro de ellas contra desastres tales como incendios, terremotos, inundaciones o explosiones.

Considerar el uso de impresoras con una función de código de uso, de modo que los generadores sean los únicos que puedan obtener sus impresos y solamente estando parados al lado de la impresora.

11.4 Control de acceso a la red

OBJETIVO: Prevenir el acceso no autorizado a los servicios en red. Debería controlarse el acceso a los servicios en red, tanto internos como externos. El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que: a) las interfaces adecuadas son puestas entre la red de la organización y redes pertenecientes a otras organizaciones, y redes publicas. b) mecanismos de autenticación apropiados son aplicados para usuarios y equipamiento. c) se exige control del acceso de los usuarios a los servicios de información.

11.4.1 Políticas sobre el uso de servicios en red

Control

Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.

Guía de implementación

Debería ser formulada una política relativa al uso de redes y servicios de red. Esta política debería cubrir:

a) las redes y servicios de red a los cuales es permitido acceder;

b) los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red;

c) los controles de gestión y procedimientos para proteger el acceso a las conexiones y servicios de red;

d) los medios utilizados para acceder a las redes y servicios de red (por ejemplo, las condiciones para permitir el acceso discado a un servicio de Internet o sistema remoto).

La política sobre el uso de servicios de red debería ser consistente con la política de control de acceso del negocio (véase el apartado 11.1).

Información adicional

Conexiones no autorizadas o inseguras a servicios de red pueden afectar a toda la organización. Este control es particularmente importante para conexiones de red a aplicaciones sensibles o críticas del negocio o de usuarios en ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas que están fuera de la gestión de seguridad y control de la organización.

11.4.2 Autenticación de usuarios para conexiones externas

Control

Deberían emplearse métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

Guía de implementación

La autenticación de usuarios remotos puede ser lograda utilizando, por ejemplo, técnicas basadas en criptografía, señales (*tokens*) de hardware, o protocolos de desafío/respuesta. Posibles implementaciones de tales técnicas pueden ser encontradas en distintas soluciones de redes privadas virtuales (*VPN*). Líneas privadas dedicadas pueden ser utilizadas para proveer seguridad del origen de la conexión.

Los procedimientos y controles de devolución de llamada, por ejemplo, módems de retorno de llamada, pueden proveer protección contra conexiones no autorizadas y conexiones no deseadas a instalaciones de procesamiento de información de la organización. Este tipo de control autentica usuarios, tratando de establecer una conexión a una red de la organización desde sitios remotos. Cuando se utilizan estos controles, una organización no debería utilizar servicios de red, que incluyan accesos discados entrantes, o si lo hacen, deberían deshabilitarse el uso de tales características para evitar debilidades asociadas con acceso discado entrante. El proceso de devolución de llamada debería asegurar que ocurra una desconexión verdadera del lado de la organización. De otro modo el usuario remoto podría mantener la línea abierta pretendiendo que la verificación de devolución de llamada ha ocurrido. Los procedimientos y controles de devolución de llamada deberían ser exhaustivamente verificados por esta posibilidad.

La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos donde son conectados a un recurso seguro de computación compartido. Técnicas criptográficas, por ejemplo, basadas en certificados, pueden ser utilizadas para la autenticación del nodo. Esto es parte de diversas soluciones basadas en una red privada virtual (*VPN*).

Deberían implementarse controles adicionales de autenticación para controlar el acceso a redes inalámbricas. En particular se debe prestar especial atención en la selección de los controles para redes inalámbricas debido a las grandes oportunidades para intercepción e inserción no detectada de trafico de red.

Información adicional

Conexiones externas habilitan potenciales ingresos no autorizados a la información del negocio, por ejemplo métodos de acceso discado. Existen diferentes tipos de autenticación, algunos de ellos proveen una mayor nivel de protección que otros, por ejemplo,métodos basados en el uso de técnicas de criptografía pueden suministrar una autenticación mas fuerte. Es importante determinar a partir de una evaluación del riesgo, el nivel de protección requerida. Esto es necesario para la selección apropiada del método de autenticación.

Un medio de conexión automática a una computadora remota puede proveer una manera de obtener un acceso no autorizado a las aplicaciones del negocio. Esto es especialmente importante si la conexión usa una red que está fuera del control de la gestión de seguridad de la organización.

11.4.3 Identificación de equipamiento en la red

Control

La identificación automática del equipamiento debería ser considerada como medio de autenticar conexiones desde equipos y ubicaciones específicas.

Guía de implementación

La identificación del equipamiento puede ser usada si es importante que la comunicación sea sólo iniciada desde un equipo o ubicación específica. Un identificador en o conectado al equipamiento puede ser utilizada para indicar si a ese equipamiento le es permitido conectarse a la red. Estos identificadores deben indicar claramente a qué red le es permitido conectarse, si existe más de una red y particularmente si estas redes son de distinta sensibilidad. Puede ser necesario considerar protección física del equipamiento para mantener la seguridad del identificador del equipo.

Información adicional

Este control puede ser completado con otras técnicas para autenticar el usuario del equipamiento (véase el apartado 11.4.2). La identificación del equipamiento puede ser aplicada adicionalmente a la autenticación del usuario.

11.4.4 Protección de los puertos de configuración y diagnóstico remoto

Control

El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estar controlado.

Guía de implementación

Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computación y el personal de soporte de hardware/software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computación o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar.

Información adicional

Muchos sistemas de computadoras, sistemas de red y sistemas de comunicación son instalados con una facilidad de diagnóstico o configuración de puertos remoto para uso de los ingenieros de mantenimiento. Si no son protegidos estos puertos de diagnóstico proveen un medio de acceso no autorizado.

11.4.5 Separación en redes

Control

Grupos de servicios de información, usuarios y sistemas de información deberían ser separados en redes.

Guía de implementación

Un método para controlar la seguridad de grandes redes es dividirlas en dominios de red lógicos separados, por ejemplo, dominios de organización de redes internas y dominios externos, cada uno protegido por un perímetro de seguridad. Un conjunto graduado de controles puede ser aplicado sobre diferentes dominios de red lógica para segregar aún más los ambientes de seguridad de redes, por ejemplo, sistemas de acceso público, redes internas y activos críticos. Los dominios deberían definirse con base en una evaluación de riesgos y en los diferentes requisitos de seguridad en cada uno de los dominios.

Tal perímetro de red puede ser implementado instalando una puerta de enlace (*gateway*) segura, entre las dos redes a ser interconectadas para controlar el acceso y flujo de la información entre los dos dominios. Esta puerta de enlace (*gateway*) debería configurarse para filtrar tráfico específico entre estos dominios (véase los apartados 11.4.6 y 11.4.7) y para bloquear el acceso no autorizado de acuerdo a la política de control de acceso de la organización (véase el apartado 11.1). Un ejemplo de este tipo de puerta de enlace (*gateway*) es lo que se conoce comúnmente como cortafuegos (*firewall*). Otro método de separación de dominios lógico es restringir el acceso a la red utilizando redes privadas virtuales para grupos de usuarios dentro de la organización.

Las redes también pueden ser separadas utilizando funcionalidades del dispositivo de red, por ejemplo conmutación de IP. Dominios separados pueden luego ser implementados controlando el flujo de datos de red utilizando capacidades de conmutación y enrutamiento tales como listas de control de acceso.

Los criterios de separación de redes en dominios debería basarse en la política de control de acceso y en los requisitos de acceso (véase el apartado 10.1) y también debería tenerse en cuenta el costo relativo y el impacto en el desempeño por la incorporación de tecnologías adecuadas de puertas de enlace (*gateway*) o de enrutamiento (véanse los apartados 11.4.6 y 11.4.7).

Además, la separación de redes debería estar basada sobre el valor y clasificación de la información almacenada o procesada en la red, niveles de confianza, o líneas de negocio de modo de reducir el impacto de una interrupción de servicio.

Debería considerarse a la separación de redes inalámbricas de las redes internas y privadas. Puesto que los perímetros de las redes inalámbricas no esta bien definido, una evaluación del riesgo debería ser realizada en tal caso para identificar controles para mantener la separación de la red (por ejemplo, una autenticación fuerte, métodos criptográficos, y selección de frecuencias).

Información adicional

Las redes están siendo extendidas en forma incremental mas allá de las tradicionales fronteras organizacionales, puesto que asociaciones de negocios pueden requerir la interconexión o compartir procesamiento de la información y recursos de redes. Tales extensiones pueden incrementar el riesgo de acceso no autorizado a los sistemas de información existentes que usan la red, alguno de los cuales puede requerir protección de otros usuarios de red por su sensibilidad o criticidad.

11.4.6 Control de conexión de red

Control

Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, la capacidad de los usuarios de conectarse a la red, debería ser restringida, en línea con la política de control de acceso y requisitos de las aplicaciones de negocio (véase el apartado 11.1).

Guía de implementación

Los derechos de acceso a la red de los usuarios debería mantenerse y actualizarse según esté requerida por la política de control de acceso (véase el apartado 11.1.1).

La capacidad de conexión de usuarios puede ser restringida a través de las puertas de enlace (*gateways*) que filtran el tráfico por medio de tablas o reglas predefinidas. Ejemplos de aplicaciones para las cuales deberían aplicarse restricciones son:

a) mensajería, por ejemplo, correo electrónico;

b) transferencia de archivos;

c) accesos interactivos;

d) accesos a aplicaciones.

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red con algunas horas del día o fechas.

Información adicional

La incorporación de controles para restringir las capacidades de conexión de los usuarios puede ser requerida por la política de control de acceso para redes compartidas, especialmente aquellas que se extienden mas allá de las fronteras organizacionales.

11.4.7 Control de enrutamiento de red

Control

Deberían implementarse controles en el enrutamiento para las redes de modo de asegurar que las conexiones entre computadoras y flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

Guía de implementación

Los controles de enrutamiento deberían basarse en mecanismos de fuente positiva y verificación de la dirección de destino.

Las puertas de enlace (*gateways*) de seguridad pueden ser usadas para validar las direcciones fuentes y destinos en puntos de control de red internos y externos si son utilizadas tecnologías proxy y/o traducción de direcciones de red. Quienes implementan deberían estar advertidos de las fortalezas y defectos de cualquier mecanismo utilizado. Los requisitos para control de enrutamiento de red deberían estar basados en la política de control de acceso (véase el apartado 11.1).

Información adicional

Las redes compartidas, especialmente aquellas que se extienden más allá de las fronteras organizacionales, pueden requerir controles de enrutamiento adicionales. Esto se aplica particularmente donde las redes son compartidas con usuarios de terceras partes (no pertenecientes a la organización).

11.5 Control de acceso al sistema operativo

OBJETIVO: Evitar el acceso no autorizado a los sistemas operativos.

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

a) autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;

b) registrar intentos exitosos y fallidos de autenticación del sistema;

c) registrar el uso de privilegios especiales del sistema;

d) emitir alarmas cuando se violan las políticas de seguridad del sistema;

e) suministrar medios adecuados para la autenticación;

f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

11.5.1 Procedimientos de conexión (log-on) seguros.

Control

El acceso a los sistemas operativos debería ser controlado mediante procedimientos de conexión (*log-on*) seguros.

Guía de implementación

El procedimiento para conectarse a un sistema operativo debería ser diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el proceso de conexión (*log-on*) debería divulgar el mínimo de información sobre el sistema, de manera de evitar proveer a un usuario no autorizado con asistencia innecesaria. Un buen procedimiento de conexión (*log-on*) debería:

a) no mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión *(log-on);*

b) desplegar un mensaje genérico advirtiendo que el sistema debería ser accedido solamente por usuarios autorizados;

c) no ofrecer mensajes de ayuda durante el proceso de conexión (*log -on*) que puedan guiar a usuarios no autorizados;

d) validar la información de conexión (*log-on*) sólo tras rellenar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicar qué parte de esos datos es correcta o no;

e) limitar el número de intentos fallidos de conexión (se recomienda tres) y considerar:

1) registrar los intentos fallidos de conexión;
2) un tiempo forzoso de espera antes de permitir un nuevo intento de conexión o su rechazo sin una autorización específica;
3) la desconexión de la comunicación de datos;
4) enviar un mensaje de alarma a la consola del sistema si se ha alcanzado el máximo número de intentos de conexión;
5) establecer el número de reintentos de contraseña en conjunción con el mínimo largo de la contraseña y el valor del sistema a ser protegido;

f) limitar los tiempos máximo y mínimo permitidos para efectuar el proceso de conexión; si se exceden, el sistema debería eliminar la conexión;

g) mostrar la siguiente información tras completar una conexión con éxito:

1) fecha y hora de la anterior conexión (*log-on*) realizada con éxito;
2) detalles de cualquier intento de conexión fallido desde el momento de la última conexión realizada con éxito.

h) no mostrar la contraseña que está siendo ingresada o considerar esconder los caracteres de la contraseña con símbolos;

i) no transmitir por una red contraseñas en texto limpio.

Información adicional

Si las contraseñas son transmitidas por una red en texto limpio durante la sesión de conexión (*log-on*), pueden ser capturadas por un programa "husmeador" de red (*"sniffer"*).

11.5.2 Identificación y autenticación del usuario

Control

Todos los usuarios deberían tener un identificador único (ID de usuario) para su uso personal exclusivo, y debería elegirse una técnica de autenticación adecuada para sustentar la identidad alegada por un usuario.

Guía de implementación

Este control debería ser aplicado a todo tipo de usuarios (incluyendo personal de soporte técnico, operadores, administradores de red, programadores de sistemas, y administradores de bases de datos).

Los identificadores de usuario (*IDs*) deberían usarse para rastrear actividades hacia el individuo responsable. Las actividades regulares de usuarios no deberían realizarse desde cuentas con privilegios.

En circunstancias excepcionales, donde hay un claro beneficio para el negocio, puede emplearse el uso de un identificador de usuario (*ID*) compartido para un grupo de usuarios o para un trabajo específico. La aprobación por la dirección debería ser documentada para tales casos. Podrían ser necesarios controles adicionales para mantener las responsabilidades.

El uso de identificadores de usuario (*IDs*) genéricos por parte de un individuo debería permitirse sólo donde las funciones accesibles o acciones llevadas a cabo por el *ID* no necesitan ser rastreadas (por ejemplo, acceso sólo de lectura), o donde hay otros controles instalados (por ejemplo, contraseña para un *ID* genérico emitida solo a una persona por vez y registro de tal instancia).

Donde se requiere autenticación fuerte y verificación de identidad, deberían usarse métodos de autenticación alternativos a las contraseñas, tales como medios criptográficos, tarjetas inteligentes (*smart cards*), señales (*tokens*) o medios biométricos.

Información adicional

Las contraseñas (véase también los apartados 11.3.1 y 11.5.3) son una forma muy común de proveer identificación y autenticación basadas en un secreto que solo el usuario conoce. Lo mismo puede lograrse también con medios criptográficos y protocolos de autenticación. La fortaleza de la identificación y autenticación de usuario debería ser acorde a la sensibilidad de la información a ser accedida.

Pueden también usarse para identificación y autenticación, objetos que los usuarios poseen tales como señales (*tokens*) de memoria o tarjetas inteligentes (*smart cards*). También puede usarse para autenticar la identidad de una persona tecnologías de autenticación biométrica que usan características o atributos únicos de un individuo. Una combinación de tecnologías y mecanismos vinculados en forma segura resultará en una autenticación más fuerte.

11.5.3 Sistema de gestión de contraseñas

Control
Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

Guía de implementación

Un sistema de gestión de contraseñas debería:

a) imponer el uso de contraseñas e identificaciones de usuario (*IDs*) individuales con el fin de establecer responsabilidades;

b) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para evitar errores al introducirlas;

c) imponer la selección de contraseñas de calidad (véase el apartado 11.3.1);

d) imponer el cambio de contraseñas (véase el apartado 11.3.1);

e) forzar a los usuarios el cambio de contraseñas temporarias en su primera conexión (*log-on*) (véase el apartado 11.2.3);

f) mantener un registro de las anteriores contraseñas utilizadas, e impedir su reutilización;

g) no mostrar las contraseñas en la pantalla cuando se están introduciendo;

h) almacenar archivos de contraseñas en lugares diferentes de los y los datos del sistema de aplicaciones;

i) almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo, cifradas o mediante algoritmo *hash*).

Información adicional

Las contraseñas son una de las principales formas de validar la autorización de un usuario para acceder a un servicio de la computadora.

Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario; en tales casos, los puntos b), d) y e) de la guía de arriba no se aplican. En la mayoría de los casos las contraseñas son seleccionadas y mantenidas por usuarios. Véase el apartado 11.3.1 para guía sobre el uso de contraseñas.

11.5.4 Utilización de las prestaciones del sistema

Control

El uso de programas utilitarios que podrían ser capaces de pasar por encima de los controles del sistema y de la aplicación debería ser restringido y controlado estrechamente.

Guía de implementación

Deberían considerarse las siguientes orientaciones para el uso de prestaciones de sistema:

a) usar procedimientos de identificación, autenticación y autorización para utilitarios del sistema;

b) separar entre utilitarios del sistema y software de aplicaciones;

c) limitar el uso de utilitarios del sistema al mínimo número de usuarios autorizados y fiables(véase también el apartado 11.2.2);

d) autorizar el uso con fines específicos de utilitarios del sistema;

e) limitar la disponibilidad de utilitarios del sistema, por ejemplo, durante un cambio autorizado;

f) registrar todo uso de utilitarios del sistema;

g) definir y documentar los niveles de autorización para utilitarios del sistema;

h) remoción o inhabilitación de todo el software basado en utilitarios y software de sistema innecesarios;

i) no poner a disposición los utilitarios de sistema a los usuarios que tienen acceso a aplicaciones en sistemas donde se requiere segregación de tareas.

Información adicional

La mayoría de las instalaciones de computadora tienen uno o más programas utilitarios de sistemas que podrían ser capaces de pasar por encima los controles de sistema y aplicación.

11.5.5 Desconexión automática de sesiones

Control

Las sesiones inactivas deberían cerrarse luego de un período definido de inactividad.

Guía de implementación

Un recurso de desconexión debería borrar la pantalla de sesión y también posiblemente más tarde, cerrar tanto la sesión de aplicación como la de red luego de un período definido de inactividad. La demora en la desconexión debería reflejar los riesgos de seguridad del área, la clasificación de la información manejada y las aplicaciones utilizadas, y los riesgos relativos a los usuarios del equipo.

Puede proveerse una forma limitada de desconexión para algunos sistemas, que borran la pantalla y previenen acceso no autorizado pero no cierra la sesión de aplicación ni la de red.

Información adicional

Este control es particularmente importante en lugares con alto riesgo, que incluye áreas públicas o externas fuera de la gestión de seguridad de la organización. Las sesiones deberían cerrarse para prevenir acceso por parte de personas no autorizadas y ataques de denegación de servicio.

11.5.6 Limitación del tiempo de conexión

Control

Deberían utilizarse restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riego.

Guía de implementación

Controles de tiempo de conexión deberían ser consideradas en aplicaciones sensibles, especialmente desde ubicaciones de alto riesgo, por ejemplo, áreas públicas o externas fuera de la gestión de seguridad de la organización. Ejemplos de tales restricciones incluyen:

a) uso de espacios de tiempo predeterminados, por ejemplo, para transmisiones de archivos en lotes (*batch*), o para sesiones interactivas regulares de corta duración;

b) la restricción de tiempos de conexión al horario normal de oficina, si no hay un requisito para trabajo en horas extras o en períodos de tiempo extendido;

c) considerar re-autenticación a intervalos.

Información adicional

La limitación del período durante el cual se permiten las conexiones a los servicios computacionales reduce la ventana de oportunidad para accesos no autorizados. Limitando la duración de sesiones activas se impide que los usuarios mantengan sesiones abiertas para prevenir re-autenticación.

11.6 Control del acceso a las aplicaciones y a la información

OBJETIVO: Evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.

Se deberían usar medios de seguridad para restringir el acceso a y en de los sistemas de aplicación.

El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados. Los sistemas de aplicación deberían:

a) controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control del acceso;

b) suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación;

c) no poner en peligro otros sistemas con los que se comparten los recursos de información.

11.6.1 Restricciones del acceso a la información

Control

El acceso a información y funciones de sistema de aplicación por parte de usuarios y personal de soporte debería estar restringido de acuerdo a la política definida de control de acceso.

Guía de implementación

Las restricciones al acceso deberían estar basadas en los requisitos de la aplicación de negocios individual. La política de control de acceso debería también ser consistente con la política de acceso organizacional (véase el apartado 11.1).

Deberían considerarse las siguientes recomendaciones para dar soporte a los requisitos de restricción de accesos:

a) proveer menús para controlar los accesos a las funciones del sistema de aplicaciones;

b) controlar los derechos de acceso de los usuarios, por ejemplo, lectura, grabación, borrado, ejecución;

c) controlar los derechos de acceso de otras aplicaciones;

d) asegurarse que las salidas de los sistemas de aplicación que procesan información sensible, sólo contienen la información relevante para el uso de la salida y se envían, únicamente, a los terminales y sitios autorizados; esto debería incluir la revisión periódica de dichas salidas para garantizar la supresión de información redundante.

11.6.2 Aislamiento de sistemas sensibles.

Control

Los sistemas sensibles deberían tener entornos informáticos dedicados (aislados).

Guía de implementación

Los siguientes puntos deberían considerarse para el aislamiento de sistemas sensibles:
a) el propietario de la aplicación debería indicar explícitamente y documentar la sensibilidad de ésta (véase el apartado 7.1.2);

b) cuando una aplicación sensible se ejecute en un entorno compartido, se deberían identificar y acordar con su propietario los sistemas de aplicación con los que compartan recursos y deberían identificarse y ser aceptados por el propietario los correspondientes riesgos de la aplicación sensible.

Información adicional

Algunos sistemas de aplicaciones son lo suficientemente sensibles a pérdida potencial por lo que ellos requieren un tratamiento especial. La sensibilidad puede indicar que el sistema de aplicación:

a) debería correr en una computadora dedicada; o

b) debería compartir recursos solo con sistemas de aplicación confiables.

El aislamiento podría lograrse usando métodos físicos o lógicos (véase también el apartado 11.4.5).

11.7 Informática móvil y trabajo remoto

OBJETIVO: Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y trabajo remoto.

La protección requerida debería ser proporcional a los riesgos que causan estas formas específicas de trabajo. Deberían considerarse los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del trabajo remoto la organización debería implantar protección en el lugar del trabajo remoto y asegurar que existen las disposiciones adecuadas para este tipo de trabajo.

11.7.1 Informática y comunicaciones móviles

Control

Se debería adoptar una política formal, y medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de recursos de informática y comunicaciones móviles.

Guía de implementación

Cuando se usan recursos de informática y de comunicaciones móviles, como por ejemplo, *notebooks*, *palmtops*, *laptops*, *smart cards*, y teléfonos móviles, debería tenerse especial cuidado para asegurar que no sea comprometida la información del negocio. La política de informática móvil debería tener en cuenta los riesgos del trabajo con dispositivos móviles en ambientes desprotegidos.

La política de informática móvil debería incluir los requisitos de protección física, controles de acceso, técnicas de criptografía, respaldos, y protección contra virus. Esta política debería también incluir reglas y consejo sobre conexión de recursos móviles a redes y orientación sobre el uso de estos recursos en lugares públicos.

Debería tenerse cuidado cuando se usan recursos de informática móvil en lugares públicos tales como salas de reuniones y otras áreas desprotegidas fuera de las instalaciones de la organización. Debería adoptarse protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos, por ejemplo, usando técnicas criptográficas (véase el apartado 12.3).

Los usuarios de estos recursos de informática móvil en lugares públicos deberían ser cuidadosos para evitar el riesgo de ser observados por personas no autorizadas. Se deberían instalar y mantener al día procedimientos contra el software malicioso (véase el apartado 10.4).

Deberían realizarse respaldos regulares de la información crítica del negocio. Debería estar disponible el equipamiento para realizar un respaldo rápido y fácil de la información. Estos respaldos deben ser provistos de la adecuada protección contra, por ejemplo, robo o pérdida de la información.

Se debería proteger debidamente el uso de dispositivos de informática móvil conectados a las redes. El acceso remoto a la información del negocio a través de redes públicas usando dispositivos móviles sólo debería tener lugar luego de la identificación y autenticación exitosa, y con los mecanismos adecuados de control de acceso (véase el apartado 11.4).

Los recursos de informática móvil deberían también estar físicamente protegidos contra robo especialmente cuando se dejan, por ejemplo, en autos y otras formas de transporte, cuartos de hotel, centros de conferencia, y lugares de reunión. Debería establecerse un procedimiento específico teniendo en cuenta requisitos legales, seguros y otros requisitos de seguridad de la organización para los casos de robo o pérdida de los dispositivos móviles. Equipos que contengan información del negocio importante, sensible, y/o crítica no deberían dejarse sin vigilancia, y de ser posible, deberían bloquearse físicamente, o deberían usarse trancas o cerrojos especiales para asegurar el equipo (véase el apartado 9.2.5).

Debería organizarse entrenamiento para personal que utiliza dispositivos móviles para cultivar su conciencia de los riesgos adicionales resultantes de esta forma de trabajo y los controles que deberían implementarse.

Información adicional

Las conexiones inalámbricas a la red desde dispositivos móviles son similares a otros tipos de conexión de red, pero tiene diferencias importantes que deberían ser consideradas cuando se identifican los controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbrica no están maduros y tienen debilidades conocidas;

b) la información almacenada en dispositivos móviles puede no ser respaldada debido al ancho de banda limitado de la red y/o porque el equipo móvil puede no estar conectado cuando están planificados los respaldos.

11.7.2 Trabajo remoto

Control

Debería desarrollarse e implementarse una política, planes operacionales y procedimientos para las actividades de trabajo remoto.

Guía de implementación

Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas de que las disposiciones de seguridad son apropiadas y que los controles están implementados, y que se cumple con la política de seguridad de la organización.

Debería establecerse protección adecuada del sitio de trabajo remoto contra, por ejemplo, el robo del equipo y la información, la divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o mal uso de instalaciones. Las actividades de trabajo remoto deberían ser tanto autorizadas como controladas por la dirección, y debería asegurarse que las disposiciones adecuadas sean adoptadas para esta forma de trabajo.

Deberían considerarse los siguientes puntos:

a) la seguridad física existente en el sitio de trabajo remoto, teniendo en cuenta la seguridad física del edificio y el ambiente local;

b) el ambiente físico de trabajo remoto propuesto;

c) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información que será accedida y el paso sobre el enlace de comunicación y la sensibilidad del sistema interno;

d) la amenaza de acceso no autorizado a información o recursos por parte de otras personas que usen el alojamiento, por ejemplo familia y amigos;

e) el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de red inalámbrica;

f) políticas y procedimientos para prevenir disputas concernientes a derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

g) acceso a equipos de propiedad privada (para chequear la seguridad de la máquina o durante una investigación), que puede ser impedida por la legislación;

h) acuerdos de licenciamiento de software que son tales que la organización podría ser responsable de licenciamiento de software de cliente en estaciones de trabajo pertenecientes en forma privada a los empleados, contratista o usuarios de terceras partes;

i) requisitos de protección anti-virus y cortafuegos (*firewalls*).

Las orientaciones y disposiciones a ser consideradas deberían incluir:

a) la provisión del equipo y mobiliario de almacenamiento adecuados para las actividades de trabajo remoto, donde el uso de equipo perteneciente en forma privada que no está bajo control de la organización, no está permitido;

b) la definición del trabajo permitido, las horas de trabajo, la clasificación de la información que puede utilizar y los sistemas y servicios internos a los que el trabajador remoto está autorizado a acceder;

c) el suministro del equipo de comunicación adecuado, incluidos los métodos para asegurar el acceso remoto;

d) la seguridad física;

e) reglas y directrices sobre el acceso de familiares y visitas al equipo y la información;

f) proporcionar el soporte y mantenimiento para el hardware y el software;

g) la provisión de seguro;

h) los procedimientos de respaldo y continuidad del negocio;

i) la auditoría y seguimiento de la seguridad;

j) la revocación de autorizaciones, derechos de acceso y devolución del equipo cuando cesen las actividades de trabajo remoto.

Información adicional

El trabajo remoto utiliza tecnología de comunicaciones para habilitar al personal trabajar en forma remota desde una ubicación fija fuera de la organización.

12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.1 Requisitos de seguridad de los sistemas de información

OBJETIVO: Asegurar que la seguridad es parte integral de los sistemas de información.

Los sistemas de información incluyen: los sistemas operativos, la infraestructura, las aplicaciones de negocio, los productos en stock, los servicios y las aplicaciones desarrolladas por usuarios. El diseño e implantación del sistema de información que apoya los procesos del negocio puede ser crucial para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar y/o implementar los sistemas de información.

Todos los requisitos de seguridad deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

12.1.1 Análisis y especificación de los requisitos de seguridad

Control

Las declaraciones de requisitos de negocio para nuevos sistemas de información, o mejoras a sistemas de información existentes deberían especificar los requisitos para controles de seguridad.

Guía de implementación

Las especificaciones de los requisitos de control deberían considerar los controles automatizados a ser incorporados al sistema de información, y la necesidad de controles manuales de apoyo. Consideraciones

similares deberían ser aplicadas evaluando paquetes de software, desarrollados o comprados, para aplicaciones de gestión.

Los requisitos de seguridad y control deberían reflejar el valor de negocio del activo de la información involucrado (véase también el apartado 7.2), y el daño potencial de negocio, que podría ser resultado de una falla o ausencia de seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para poner en práctica la seguridad deberían ser integrados en las etapas tempranas de proyectos de sistema de información. Los controles introducidos en la etapa de diseño son considerablemente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si los productos son comprados, un proceso formal de pruebas y de adquisición debería ser seguido. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados. Cuando la funcionalidad de seguridad en un producto propuesto no satisface el requisito especificado entonces el riesgo introducido y los controles asociados deberían ser reconsiderados antes de la compra del producto. Cuando una funcionalidad adicional es suministrada y causa un riesgo de seguridad, esta debería ser deshabilitada o la estructura de control propuesta debería ser revisada para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

Información adicional

Si se considera apropiado, por ejemplo por motivos de costo, la dirección puede desear utilizar productos evaluados y certificados independientemente. Información adicional sobre criterios de evaluación para productos de seguridad de TI puede ser encontrada en la norma ISO/IEC 15408 o en otras normas de evaluación o de certificación, según sea apropiado.

La norma ISO/IEC TR 13335-3 proporciona guías sobre el empleo de procesos de gestión de riesgos para identificar requisitos para controles de seguridad.

12.2 Procesamiento correcto en las aplicaciones

OBJETIVO: Prevenir errores, pérdida, modificación no autorizada o mal uso de información en aplicaciones.

En las aplicaciones deberían ser diseñados controles apropiados, incluyendo en las aplicaciones desarrolladas por usuarios para asegurar el tratamiento correcto. Estos controles deberían incluir la validación de datos de entrada, el tratamiento interno y datos de salida.

Los sistemas que procesan, o tienen impacto sobre, la información sensible, valiosa o crítica pueden requerir controles adicionales. Tales controles deberían ser determinados sobre la base de requisitos de seguridad y evaluación del riesgo.

12.2.1 Validación de datos de entrada

Control

Los datos de entrada a aplicaciones deberían ser validados para asegurar que estos datos son correctos y apropiados.

Guía de implementación

Deberían ser aplicadas comprobaciones a la entrada de transacciones de negocio, datos permanentes (por ejemplo nombres y direcciones, límites de crédito, números de referencia de cliente), y mesas de parámetro

(por ejemplo, precios de las ventas, tarifas monetarias de conversión, tarifas fiscales). Las directrices siguientes deberían ser consideradas:

a) entrada duplicada u otras comprobaciones de entrada, como:

1) valores fuera de rango;
2) caracteres inválidos en campos de datos;
3) pérdida o datos incompletos;
4) exceder límites superiores e inferiores de volumen de datos;
5) datos de control no autorizados o incoherentes;

b) la revisión periódica del contenido de campos clave o archivos de datos para confirmar su validez e integridad;

c) la inspección de documentos físicos de entrada por si introducen cualquier cambio no autorizado (todos los cambios a documentos de entrada deberían ser autorizados);

d) procedimientos para responder a errores de validación;

e) procedimientos para probar la plausibilidad de los datos de entrada;

f) definición de las responsabilidades de todo el personal implicado en el proceso de entrada de datos;

g) la creación de un registro de las actividades implicadas en el proceso de entrada de datos (véase el apartado 10.10.1).

Información adicional

El examen automático y la validación de datos de entrada pueden ser considerados, como aplicables, para reducir el riesgo de errores y prevenir ataques estándar incluyendo desbordamiento de buffer (*buffer overflow*) e inyección de códigos (*code injection*).

12.2.2 Control de procesamiento interno

Control

Las comprobaciones de validación deberían ser incorporadas en las aplicaciones para descubrir cualquier corrupción de información por errores de procesamiento o actos deliberados.

Guía de implementación

El diseño y la implementación de aplicaciones deberían asegurar que los riesgos de procesar errores que conducen a una pérdida de integridad son reducidos al mínimo.

Áreas específicas a considerar incluyen:

a) el empleo de las funciones agregar, modificar, y suprimir para implementar cambios a datos;

b) procedimientos para prevenir programas que corran en el orden incorrecto o luego del error de un proceso previo (véase también el apartado 10.1.1);

c) el empleo de programas apropiados para reponerse de errores y asegurar el tratamiento correcto de datos;

d) la protección contra ataques que usan el desbordamiento / exceso en el *buffer*.

Se deberían elaborar listas de verificación adecuadas, documentar las actividades y mantener seguros los resultados. Ejemplos de las comprobaciones que pueden ser incorporadas incluyen lo siguiente:

a) controles de sesión o de lotes para conciliar balances después de la actualización de transacciones;

b) controles de balance para, para comprobar los balances de apertura contra los balances anteriores de cierre, a saber:

1) controles de ejecución a ejecución;
2) totales de actualización de archivos;
3) controles de programa a programa;

c) la validación de datos de entrada generados por el sistema (véase el apartado 12.2.1);

d) comprobar la integridad, la autenticidad o cualquier otro rasgo de seguridad de datos o software transferido desde o hacia, entre ordenadores centrales y remotos;

e) los totales de verificación (*hash*) de registros y archivos;

f) comprobaciones para asegurar que los programas de aplicación se ejecutan en el tiempo correcto;

g) comprobaciones para asegurar que los programas son ejecutados en el orden correcto, que se terminan en caso de una falla y que el tratamiento remoto es detenido hasta que el problema sea resuelto;

h) la creación de un registro de las actividades implicadas en el tratamiento (véase el apartado 10.10.1).

Información adicional

Los datos que han sido ingresados correctamente pueden ser corrompidos por errores de hardware, errores de procesamiento o por actos deliberados. Las comprobaciones de validación requeridas dependerán de la naturaleza de la aplicación y el impacto al negocio de cualquier corrupción de datos.

12.2.3 Integridad del mensaje

Control

Deberían identificarse los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles apropiados.

Guía de implementación

Una evaluación de riesgos de seguridad debería ser realizada para determinar si requiere la integridad del mensaje e identificar el método más apropiado de implementación.

Información adicional

Técnicas criptográficas (véase el apartado 12.3) pueden ser utilizadas como un medio apropiado de implementar la autenticación del mensaje.

12.2.4 Validación de los datos de salida

Control

La salida de datos de una aplicación debería ser validada para asegurar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias.

Guía de implementación

La validación de salida puede incluir:

a) validaciones de verosimilitud para comprobar si los datos de salida son razonables;

b) cuentas de control de reconciliación para asegurar el tratamiento de todos los datos;

c) suministro de información suficiente para un lector o sistema de procesamiento subsecuente para determinar la exactitud, entereza, precisión, y clasificación de la información;

d) procedimientos para responder a pruebas de validación de salida;

e) definición de las responsabilidades de todo el personal implicado en el proceso de salida de datos;

f) creación de un registro de actividades en el proceso de validación de salida de datos.

Información adicional

Típicamente los sistemas y aplicaciones son construidos suponiendo que habiendo emprendido la validación apropiada, la verificación, y pruebas, la salida siempre es correcta. Sin embargo, esta suposición no es siempre válida; es decir, sistemas que han sido probados pueden producir todavía en algunas circunstancias una salida incorrecta.

12.3 Controles criptográficos

OBJETIVO: Proteger la confidencialidad, autenticidad o integridad de información por medios criptográficos. Debería desarrollarse una política sobre el empleo de controles criptográficos y establecerse una gestión de claves para dar soporte al empelo de técnicas criptográficas.

12.3.1 Política sobre el empleo de controles criptográficos

Control

Debería ser desarrollada e implementada una política sobre el empleo de controles criptográficos para la protección de información.

Guía de implementación

Cuando se desarrolla una política sobre el empleo de controles criptográficos lo siguiente debería ser considerado:

a) el enfoque de la dirección hacia el empleo de controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales la información de negocio debería ser protegida (véase también el apartado 5.1.1);

b) basado en una evaluación de riesgo, el nivel requerido de protección debería ser identificado teniendo en cuenta el tipo, la fuerza, y la calidad del algoritmo de cifrado requerido;

c) el empleo de cifrado para protección de información sensible transportada por medios de comunicación móviles o removibles, por dispositivos o a través de líneas de comunicación;

d) un enfoque de gestión de claves, incluyendo métodos para tratar la protección de claves criptográficas y la recuperación de información cifrada en el caso de claves perdidas, comprometidas o dañadas;

e) funciones y responsabilidades, por ejemplo, quién es responsable de:

1) la implementación de la política;
2) la gestión de la clave, incluyendo la generación de la clave (véase también el apartado 12.3.2);

f) las normas a ser adoptadas para la implementación eficaz en todas partes de la organización (que solución usar para que proceso de negocio);

g) el impacto de usar información cifrada, sobre los controles que confían en la inspección de contenido (por ejemplo la detección de virus).

Al implementar la política criptográfica de la organización, deberían considerarse las regulaciones y las restricciones nacionales que podrían aplicarse al empleo de técnicas criptográficas en las diferentes partes del mundo y las cuestiones de pasaje de frontera de transacciones de información cifrada (véase también el apartado 15.1.6).

Los controles criptográficos pueden ser usados para alcanzar diferentes objetivos de seguridad, por ejemplo:

a) confidencialidad: utilización de cifrado de información para proteger información sensible o crítica, almacenada o transmitida;

b) integridad/autenticidad: la utilización de firmas digitales o códigos de autenticación de mensaje para proteger la autenticidad y la integridad de la información sensible o crítica almacenada o transmitida;

c) no repudio: utilización de técnicas criptográficas para obtener pruebas del suceso o no de un acontecimiento o acción.

Información adicional

La toma de una decisión en cuanto a si una solución criptográfica es apropiada debería ser vista como parte del proceso más amplio de evaluación de riesgo y selección de control. Esta evaluación puede entonces ser usada para determinar si un control criptográfico es apropiado, qué tipo del control debería ser aplicado y para que objetivo y proceso de negocio. Una política sobre el empleo de controles criptográficos es necesaria para maximizar las ventajas y reducir al mínimo los riesgos de usar técnicas criptográficas, y evitar el empleo inadecuado o incorrecto. Usando firmas digitales, deberían dar consideración a cualquier legislación relevante, en particular la legislación que describe las condiciones en las cuales una firma digital obliga legalmente (véase el apartado 15.1).

Debería buscarse la asesoría de un especialista para identificar el nivel apropiado de protección y definir las especificaciones convenientes que proporcionarán la protección requerida y apoyarán la implementación de un sistema de gestión de clave seguro (véase también el apartado 12.3.2).

El comité conjunto ISO/IEC JTC1 SC27 ha desarrollado varias normas relacionadas con controles criptográficos. También puede ser encontrada información adicional en la norma IEEE P1363 y en las directrices OECD sobre criptografía.

12.3.2 Gestión de claves

Control

Debería establecerse la gestión de claves para apoyar el uso de técnicas criptográficas en la organización.

Guía de implementación

Todas las claves criptográficas deberían ser protegidas contra la modificación, la pérdida, y la destrucción. Además, claves secretas y privadas necesitan la protección contra el descubrimiento no autorizado. El equipo para generar, almacenar y archivar claves debería ser protegido físicamente.

Un sistema de gestión de claves debería estar basado en un conjunto reconocido de normas, procedimientos, y métodos seguros para:

a) generar claves para sistemas criptográficos diferentes y aplicaciones diferentes;

b) generar y obtener certificados de clave pública;

c) distribuir claves a los usuarios que corresponda, incluyendo cómo deberían activarse las claves al recibirse;

d) almacenar claves, incluyendo cómo los usuarios autorizados obtienen el acceso a las claves;

e) cambiar o actualizar claves , incluyendo reglas sobre cuándo las claves deberían ser cambiadas y cómo esto debería hacerse;

f) tratar las claves comprometidas;

g) revocar claves incluyendo cómo deberían retirarse o desactivarse las mismas, por ejemplo, cuando las claves están comprometidas o cuando un usuario se desvincula de la organización (en cuyo caso las claves también deberían archivarse);

h) recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio, por ejemplo, para recuperar la información cifrada;

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 las claves.

Para reducir la probabilidad de compromiso, la activación, y fechas de desactivación de claves deberían ser definidas de modo que las claves sólo puedan ser usadas durante un período limitado de tiempo. Este período de tiempo debería ser dependiente de las circunstancias en las cuales el control criptográfico es usado, y el riesgo percibido.

Además de la gestión segura de claves públicas y privadas, la protección de claves públicas también debería ser considerada.

Este proceso de autenticación puede ser hecho usando los certificados de clave pública que normalmente son emitidos por una autoridad de certificación, que debería ser una organización aprobada con controles y procedimientos adecuados para proporcionar el grado de confiabilidad requerido.

El contenido de los acuerdos de nivel de servicio o de los contratos con los proveedores de servicios criptográficos (por ejemplo, una autoridad certificadora) debería cubrir los aspectos de las obligaciones y responsabilidades, fiabilidad de los servicios y tiempos de respuesta para su suministro (véase el apartado 6.2.3).

Información adicional

La gestión de claves criptográficas es esencial para el empleo eficaz de técnicas criptográficas. ISO/IEC 11770 proporciona información adicional sobre la gestión de clave. Los dos tipos de técnicas criptográficas son:

a) técnicas de claves secretas, donde dos o más partes comparten la misma clave y esta clave es usada tanto para cifrar como descifrar la información; esta clave debería mantenerse secreta puesto que cualquiera que tenga acceso a ella puede descifrar toda la información cifrada con dicha clave, o introducir información no autorizada con esa clave;

b) técnicas de clave pública, donde cada usuario tiene un par de claves, una clave pública (que puede ser revelada a alguien) y una clave privada (que tiene que ser mantenida secreta); Las técnicas de clave pública pueden ser usadas para el cifrado y producir firmas digitales (véase también las normas ISO/IEC 9796 e ISO/IEC 14888).

Existe la amenaza de falsificar una firma digital substituyendo la clave pública de un usuario. Este problema es manejado con el empleo de certificado de clave pública.

Las técnicas criptográficas también pueden ser usadas para proteger claves criptográficas. Puede ser necesario considerar procedimientos para manejar demandas legales por el acceso a claves criptográficas, por ejemplo, información cifrada puede tener que estar disponible en forma no cifrada como prueba en un caso judicial.

12.4 Seguridad de los archivos del sistema

OBJETIVO: Garantizar la seguridad de los archivos del sistema. El acceso a archivos del sistema y el código original de programa debería ser controlado, y los proyectos de tecnología de la información y las actividades de apoyo conducidas en una manera segura. Debería tomarse el cuidado para evitar la exposición de datos sensibles en ambientes de prueba.

12.4.1 Control de software en producción

Control

Debería haber procedimientos para controlar la instalación de software sobre sistemas en producción.

Guía de implementación

Para reducir al mínimo el riesgo de corrupción en sistemas en producción, las directrices siguientes, deberían ser consideradas en el control de cambio:

a) la actualización de software en producción, aplicaciones, y bibliotecas de programa sólo debería ser realizada por administradores entrenados con la apropiada autorización de la dirección (véase el apartado 12.4.3);

b) Los sistemas en producción deberían tener sólo código ejecutable aprobado y no código de desarrollo o compiladores;

c) El software de aplicaciones y el de sistemas operativos deberían ser implementados sólo después de pruebas extensas y acertadas; las pruebas deberían incluir pruebas sobre la utilidad, la seguridad, efectos sobre otros sistemas y facilidades de usuario, y deberían ser realizadas sobre sistemas separados (véase también el apartado 10.1.4); debería asegurarse que todas las bibliotecas de programas fuentes correspondientes han sido actualizadas;

d) debería utilizarse un sistema de control de configuración para mantener el control de todo el software implementado así como la documentación de sistema;

e) debería existir una estrategia de “vuelta atrás” antes de que los cambios sean implementados;

f) debería mantenerse un registro de auditoría de todas las actualizaciones a las bibliotecas de programa en producción;

g) debería conservarse la versión anterior de software de aplicación como una medida de contingencia;

h) deberían archivarse las versiones viejas de software, junto con toda la información requerida y parámetros, procedimientos, detalles de configuración, y el software de apoyo mientras los datos son conservados en el archivo.

El software utilizado en producción suministrado por vendedores debería mantener un nivel de servicio apoyado por el proveedor. Con el tiempo, los vendedores de software dejarán de dar soporte a las versiones más viejas de software. La organización debería considerar los riesgos de confiar en el software sin soporte.

Cualquier decisión de cambio a una nueva versión debería tener en cuenta para el cambio, los requisitos del negocio y la seguridad de la nueva versión, por ejemplo la introducción de una nueva funcionalidad de seguridad o el número y la severidad de problemas de seguridad que afectan esta versión. Los parches de software deberían aplicarse cuando puedan ayudar a quitar o reducir debilidades de seguridad (véase también el apartado 12.6.1).

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedor deberían ser supervisadas.

El software de computador puede depender de software y módulos suministrados externamente, lo cual se debería supervisar y controlar para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

Información adicional

Sólo deberían cambiarse los sistemas operativos cuando hay un requisito para hacer, por ejemplo, si la versión actual del sistema operativo no soporta las exigencias de negocio. Las mejoras no deberían ocurrir solamente porque una nueva versión del sistema operativo está disponible. Las nuevas versiones de sistemas operativos pueden ser menos seguras, menos estables, y menos entendidas que los sistemas actuales.

12.4.2 Protección de datos de prueba del sistema

Control

Los datos de prueba deberían ser seleccionados cuidadosamente, protegidos y controlados.

Guía de implementación

Para hacer pruebas debería ser evitado el empleo de bases de datos de producción que contienen información personal o cualquier otra información sensible. Si se utiliza información personal o cualquier otra información sensible para hacer pruebas, todos los detalles y el contenido sensible deberían ser eliminados o modificados, más allá del reconocimiento, antes del empleo. Las directrices siguientes deberían ser aplicadas para proteger datos de producción cuando son utilizados para hacer pruebas:

a) los procedimientos de control de acceso, que se aplican a sistemas de aplicaciones en producción, deberían aplicarse también a los sistemas de prueba de aplicaciones;

b) debería autorizarse por separado, cada vez que se copie la información de producción a un sistema de prueba de aplicación;

c) debería borrarse, la información de producción de un sistema de prueba de aplicación inmediatamente después de que las pruebas son completadas;

d) debería registrarse, la copia y el empleo de información de producción para proporcionar una pista de auditoría.

Información adicional

Las pruebas de sistema y de aceptación requieren por lo general volúmenes sustanciales de datos de prueba que sean tan cercanos como sea posible a datos de producción.

12.4.3 Control de acceso al código de programas fuente

Control

El acceso al código de programas fuente debería ser restringido.

Guía de implementación

El acceso al código de programas fuente y artículos asociados (como diseños, datos específicos, proyectos de verificación y proyectos de validación) debería ser estrictamente controlado, para prevenir la introducción de funcionalidad no autorizada y evitar cambios involuntarios. Para el código de programas fuente, esto puede alcanzarse por el almacenamiento centralizado, controlado de tal código, preferentemente en bibliotecas de programas fuente. Las directrices siguientes deberían ser consideradas (véase también la cláusula 11) para controlar el acceso a tales bibliotecas de programas fuente y para reducir el potencial de corrupción de programas del computador:

a) de ser posible, las bibliotecas de programas fuente no deberían ser soportadas en sistemas de producción;

b) el código de programas fuente y las bibliotecas de programas fuente deberían gestionarse según procedimientos establecidos;

c) el personal de apoyo debería tener acceso restringido a bibliotecas de programas fuente;

d) la actualización de bibliotecas de programas fuente y artículos asociados, y la entrega de programas fuente a programadores sólo debería realizarse después de que la autorización apropiada ha sido recibida;

e) los listados de programas deberían mantenerse en un ambiente seguro (véase el apartado 10.7.4);

f) debería mantenerse un registro de auditoría de todos los accesos a bibliotecas de programas fuente;

g) el mantenimiento y la copia de bibliotecas de programas fuente deberían estar sujetos a procedimientos estrictos de control de cambio (véase el apartado 12.5.1).

Información adicional

El código de programas fuente es el código escrito por programadores, que son compilados (y enlazados) para crear ejecutables. Ciertos lenguajes de programación, como el ejecutable es creado en el tiempo en que es activado no distinguen formalmente entre el código fuente y ejecutable.

Las normas ISO 10007 e ISO/IEC 12207 proporcionan información adicional sobre los procesos de gestión de configuración y el proceso de ciclo de vida del software.

12.5 Seguridad en los procesos de desarrollo y soporte

OBJETIVO: Mantener la seguridad del software de aplicación e información. Los proyectos y ambientes de soporte deberían controlarse estrictamente. Los gerentes responsables de sistemas de aplicación también deberían ser responsables de la seguridad del proyecto o ambiente de soporte. Ellos deberían asegurar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del ambiente de producción.

12.5.1 Procedimientos de control de cambio

Control

La implementación de cambios debería controlarse mediante el empleo de procedimientos formales de control de cambio.

Guía de implementación

Para reducir al mínimo la corrupción de sistemas de información, deberían documentarse y hacerse cumplir procedimientos formales de control de cambio. La introducción de nuevos sistemas y cambios mayores a sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad, y gestión de implementación.

Este proceso debería incluir una evaluación de riesgo, el análisis de los impactos de cambios, y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurar que los procedimientos existentes de seguridad y control no son comprometidos, que a los programadores de apoyo se les da el acceso sólo a aquellas partes del sistema necesario para su trabajo, y que el acuerdo formal y la aprobación para cualquier cambio son obtenidos.

De ser practicable, los procedimientos de control de cambio de aplicación y operacionales deberían integrarse (véase también el apartado 10.1.2). Los procedimientos de cambio deberían incluir:

a) el mantenimiento de un registro de niveles de autorización acordados;

b) asegurar que los cambios son efectuados por usuarios autorizados;

c) revisar los controles y procedimientos de integridad para asegurar que no serán comprometidos por los cambios;

d) identificar todo el software, la información, entidades de base de datos, y el hardware que requieran enmienda;

e) obtener la aprobación formal para propuestas detalladas antes de que comience el trabajo;

f) asegurar que los usuarios autorizados acepten los cambios antes de la implementación;

g) asegurar que al terminar cada cambio la documentación de sistema es actualizada y que la vieja documentación es archivada o eliminada;

h) el mantenimiento de una versión controlada de todas las actualizaciones de software;

i) el mantenimiento de una pista de auditoría de todo el cambio solicitado;

j) asegurar que la documentación de operaciones (véase el apartado 10.1.1) y los procedimientos de usuario son cambiados según es necesario para permanecer adecuada;

k) asegurar que la implementación de cambios ocurra en el momento adecuado y no interfiera los procesos de negocio implicados.

Información adicional

El cambio del software puede afectar el ambiente de producción.

Las buenas prácticas incluyen las pruebas del software nuevo en un ambiente segregado tanto del ambiente de producción como del ambiente de desarrollo (véase también el apartado 10.1.4). Esto proporciona un medio para tener el control sobre el nuevo software y permitir protección adicional a la información de producción que es utilizada para hacer pruebas. Esto debería incluir parches, paquetes de servicio (*service packs*), y otras actualizaciones. Las actualizaciones automatizadas no deberían ser usadas sobre sistemas críticos ya que algunas actualizaciones pueden hacer que fallen aplicaciones críticas (véase el apartado 12.6).

12.5.2 Revisión técnica de aplicaciones después de cambios del sistema operativo

Control

Cuando los sistemas operativos son cambiados, las aplicaciones críticas del negocio deberían ser revisadas y probadas para asegurar que no hay ningún impacto adverso sobre las operaciones o seguridad de la organización.

Guía de implementación

Este proceso debería cubrir:

a) la revisión de los controles de aplicación y procedimientos de integridad para asegurar que ellos no han sido comprometidos por los cambios de sistema operativo;

b) asegurar que el plan de apoyo anual y el presupuesto cubrirán pruebas y revisiones de sistema resultantes de los cambios de sistema operativo;

c) asegurar que la notificación de cambios al sistema operativo es proporcionada a tiempo para permitir que ocurran pruebas y revisiones apropiadas antes de la puesta en producción;

d) asegurar que los cambios apropiados son hechos en los planes de continuidad de negocio (véase la cláusula 14).

Debería darse a un grupo o individuo específico la responsabilidad de supervisar vulnerabilidades y las liberaciones de parches y actualizaciones de los vendedores (véase el apartado 12.6).

12.5.3 Restricciones sobre cambios a paquetes de software

Control

Las modificaciones a paquetes de software deberían ser desalentadas, limitadas a cambios necesarios, y todos los cambios deberían ser estrictamente controlados.

Guía de implementación

En la medida de lo posible, y practicable, los paquetes de software, suministrados por vendedores deberían ser utilizados sin modificación. Cuando un paquete de software necesite ser modificado los siguientes puntos deberían ser considerados:

a) el riesgo de comprometer los procesos de control y de integridad existentes;

b) si el consentimiento del vendedor debería ser obtenido;

c) la posibilidad de obtener los cambios requeridos del vendedor como actualizaciones normales de programa estándar;

d) el impacto ocasionado, si la organización se hace responsable por el futuro mantenimiento del software como consecuencia de los cambios.

Si los cambios son necesarios el software original sería conservado y los cambios aplicados a una copia claramente identificada. Un proceso de gestión de actualización de software debería ser puesto en práctica para asegurar que los parches más actualizados aprobados y actualizaciones de aplicación son instaladas para todo el software autorizado (véase el apartado 12.6). Todos los cambios totalmente deberían ser probados y documentados, de modo que ellos puedan ser vueltos a aplicar si fuera necesario a futuras mejoras de software.

De ser requerido, las modificaciones deberían ser probadas y validadas por un equipo de evaluación independiente.

12.5.4 Fuga de Información

Control

Deberían prevenirse las oportunidades para la fuga de la información.

Guía de implementación

Para limitar el riesgo de fugas de información, por ejemplo, por el empleo y la explotación de canales encubiertos, debería considerarse lo siguiente:

a) explorar los medios de comunicación de salida y comunicaciones de información oculta;

b) enmascaramiento y modulación de sistemas y comportamiento de comunicaciones para reducir la probabilidad de que un tercero sea capaz de deducir información de tal comportamiento;

c) aprovechando sistemas y software que son considerados, de alta integridad, por ejemplo usando productos evaluados (véase la norma ISO/IEC 15408);

d) donde sea permitido, supervisión regular de personal y actividades de sistema, conforme a legislación o regulación existente;

e) supervisión de uso de recurso en sistemas de computador.

Información adicional

Los canales encubiertos son los caminos que no son queridos para conducir flujos de la información, pero que sin embargo pueden existir en un sistema o la red. Por ejemplo, manipular bits en protocolos de comunicación de paquetes podría ser usado como un método oculto de señalización. Por naturaleza, prevenir la existencia de todos los posibles canales encubiertos sería difícil, si no imposible. Sin embargo, la explotación de tales canales es a menudo realizada por el código troyano (véase también el apartado

10.4.1). Por lo tanto la toma de medidas para proteger contra el código troyano reduce el riesgo de explotación de canal encubierto.

La prevención acerca de accesos de red no autorizados (11.4), así como la política y los procedimientos para desalentar el mal uso de servicios de la información por el personal (15.1.5), ayudará a protegerse contra canales encubiertos.

12.5.5 Desarrollo externo de software

Control

El desarrollo externo de software debería ser supervisado y seguido por la organización.

Guía de implementación

Cuando el desarrollo de software sea externo, los siguientes puntos deberían considerarse:

a) acuerdos de licencias, la propiedad del código, y derechos de propiedad intelectual (véase el apartado 15.1.2);

b) certificación de la calidad y exactitud del trabajo realizado;

c) acuerdos de custodia (*escrow*) en caso de fracaso del proveedor externo;

d) los derechos de acceso para la revisión de la calidad y exactitud de trabajo realizado;

e) exigencias contractuales sobre la calidad y seguridad de la funcionalidad del código;

f) pruebas antes de la instalación para descubrir código malicioso y troyano.

12.6 Gestión de vulnerabilidad técnica

OBJETIVO: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas. La gestión de vulnerabilidades técnicas debería implementarse como un camino eficaz, sistemático, y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir los sistemas operativos, y cualquier otra aplicación en uso.

12.6.1 Control de vulnerabilidades técnicas

Control

Debería obtenerse información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a tales vulnerabilidades, y tomar medidas apropiadas para gestionar el riesgo asociado.

Guía de implementación

Un requisito previo para la gestión eficaz de vulnerabilidades técnicas es un inventario actual y completo de activos (véase el apartado 7.1). Información específica necesaria para apoyar la gestión de vulnerabilidades técnicas, incluye al vendedor de software, números de versión, el estado actual de despliegue (por ejemplo qué software esté instalado sobre qué sistemas), y la(s) persona(s) responsable(s) dentro de la organización del software.

Apropiadamente, la acción oportuna debería tomarse en respuesta a la identificación de potenciales vulnerabilidades técnicas. Las siguientes recomendaciones deberían seguirse para establecer un proceso eficaz de gestión de vulnerabilidades técnicas:

a) la organización debería definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo la supervisión de la vulnerabilidad, la evaluación de riesgo de la vulnerabilidad, la aplicación de parches (*patchs*), el seguimiento de activo, y cualquier responsabilidad de coordinación requerida;

b) deberían identificarse los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (basado a la lista de inventario de activos, véase el apartado 7.1.1), estos recursos de la información deberían ser actualizados basándose en cambios del inventario, o cuando son encontrados otros recursos nuevos o útiles;

c) un cronograma para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

d) una vez que ha sido detectada una potencial vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las acciones a ser tomadas; tal acción podría implicar el instalar el parche (*patch*) a sistemas vulnerables y/o la aplicación de otros controles;

e) según cuán urgentemente tiene que ser gestionada una vulnerabilidad técnica, la acción a tomar debería ser realizada según controles relacionados a la gestión de cambio (véase el apartado 12.5.1) o según procedimientos de gestión de incidentes de seguridad de la información (véase el apartado 13.2);

f) si está disponible un parche (*patch*), los riesgos asociados con la instalación del parche (*patch*) deberían ser evaluados (los riesgos planteados por la vulnerabilidad deberían ser comparados con el riesgo de instalar el parche);

g) los parches (*patches*) deberían probarse y evaluarse antes de ser instalados para asegurarse que son eficaces y no causan efectos secundarios que no pueden ser tolerados; si no está disponible ningún parche, deberían considerarse otros controles, como:

1) bajar servicios o funcionalidades relacionadas con la vulnerabilidad;
2) adaptar o agregar controles de acceso, por ejemplo: cortafuegos (firewalls), en los bordes de la red (véase el apartado 11.4.5);
3) aumentar el seguimiento para descubrir o prevenir ataques reales;
4) fomentar conciencia de la vulnerabilidad;

h) debería mantenerse un registro de auditoría para todos los procedimientos emprendidos;

i) debería supervisarse y evaluarse con regularidad el proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficacia;

j) deberían gestionarse primero los sistemas en alto riesgo.

Información adicional

El correcto funcionamiento del proceso de gestión de vulnerabilidades técnicas de una organización es crítico en muchas organizaciones y por lo tanto debería ser supervisado con regularidad. Un inventario exacto es esencial para asegurar que son identificadas vulnerabilidades técnicas potencialmente relevantes.

La gestión de vulnerabilidades técnicas puede ser vista como una sub-función de la gestión de cambio y como tal puede aprovechar los procesos y procedimientos de gestión de cambio (véase los apartados 10.1.2 y 12.5.1).

Los vendedores están a menudo bajo la presión significativa de liberar parches (*patches*) cuanto antes. Por lo tanto, un parche (*patch*) puede no gestionar el problema adecuadamente y puede tener efectos secundarios negativos. También, en algunos casos, una vez que el parche (*patch*) es aplicado, puede no ser fácilmente efectuada la desinstalación del mismo.

Si no son posibles las pruebas adecuadas de los parches, por ejemplo, debido a gastos o carencia de recursos, puede considerarse, una demora en aplicar el parche (*patch*), para evaluar los riesgos asociados, basados en la experiencia reportada por otros usuarios

13 Gestión de incidentes de la seguridad de la información

13.1 Reporte de debilidades y eventos de seguridad de la información

OBJETIVO: Asegurar que las debilidades y eventos de seguridad de la información asociados a sistemas de información son comunicados de manera de permitir tomar acciones correctivas a tiempo.

Deberían establecerse procedimientos formales de reporte y escalamiento de eventos. Todos los empleados, contratistas y usuarios de terceras partes deberían ser puestos al tanto de los procedimientos para reportar los diversos tipos de acontecimientos y debilidades que puedan tener un impacto en la seguridad de activos de la organización. A ellos se les debería exigir reportar cualquier evento o debilidad de seguridad de la información lo más rápidamente posible al punto designado de contacto.

13.1.1 Reportando eventos de seguridad de la información

Control

Los eventos de seguridad de la información deberían ser reportados a través de los canales apropiados de gestión tan pronto como sea posible.

Guía de implementación

Debería establecerse un procedimiento formal para el reporte de eventos de seguridad de la información, junto con una respuesta al incidente y un procedimiento de escalamiento, precisando la acción que se tomará al momento de recibir un informe de un evento de seguridad de la información. Debería establecerse un punto de contacto para el reporte de los eventos de seguridad de la información. Debería asegurarse que este punto de contacto se conoce en toda la organización, está siempre disponible y puede proporcionar respuesta adecuada y oportuna.

Todos los empleados, contratistas y usuarios de terceros deberían ser advertidos de su responsabilidad de reportar cualquier evento de seguridad de la información lo más rápidamente posible. Deberían también conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir:

a) procesos adecuados de realimentación para asegurarse de aquellos que reportan eventos de seguridad de la información están siendo notificados de los resultados después que el reporte se haya tratado y haya sido cerrado;

b) formatos para el reporte de eventos de seguridad de la información como forma de soporte a la acción de generación de reportes, y para ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información;

c) el comportamiento correcto que se emprenderá en caso de un evento de seguridad de la información, es decir:

1) observando todos los detalles importantes (por ejemplo, tipo del incumplimiento o violación, mal funcionamiento que se presenta, mensajes en la pantalla, comportamiento extraño) inmediatamente;
2) no realizando ninguna acción propia, pero inmediatamente reportar al punto de contacto;

d) referencia a un proceso disciplinario formal establecido para tratar con empleados, contratistas o usuarios de terceros que cometen eventos de seguridad.

En ambientes de alto riesgo, una alarma de coerción[4] puede ser proporcionada mediante la cual una persona bajo coerción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coerción deberían reflejar la situación de alto riesgo que tales alarmas están indicando.

Información adicional

Ejemplos de eventos e incidentes de seguridad de la información son:
a) pérdida de servicio, de equipos o de instalaciones;

b) mal funcionamiento o sobrecargas del sistema;

c) errores humanos;

d) no cumplimiento con políticas o pautas;

e) violaciones de las disposiciones de seguridad física;

f) cambios de sistema no controlados;

g) mal funcionamiento de software o hardware;

h) violaciones de acceso.

Con el debido cuidado de los aspectos de confidencialidad, los incidentes de seguridad de la información se pueden utilizar en la formación de conciencia del usuario (véase el apartado 8.2.2) como ejemplos de lo que podría suceder, cómo responder a tales incidentes, y cómo evitarlos en el futuro. Para poder atender eventos e incidentes de seguridad de la información podría ser necesario recoger evidencia cuanto antes después de la ocurrencia (véase el apartado 13.2.3).

Los desperfectos u otros comportamientos anómalos del sistema pueden ser un indicador de un ataque a la seguridad o de una violación real a la seguridad y por lo tanto debería siempre reportarse como un evento de seguridad de la información.

Más información sobre el reporte de eventos de seguridad de la información y gestión de los incidentes de seguridad de la información se puede encontrar en la norma ISO/IEC TR 18044.

13.1.2 Reportando debilidades de seguridad

[4] una alarma de coerción es un método para secretamente indicar que una acción está ocurriendo bajo coerción.

Control

A todos los empleados, contratistas y usuarios de terceros de sistemas y de los servicios de información se les debería exigir observar y reportar cualquier debilidad de seguridad vista o sospechada en sistemas o servicios.

Guía de implementación

Todos los empleados, contratistas y usuarios de terceros deberían reportar estos asuntos ya sea a su gerencia o directamente a su proveedor de servicios lo más rápidamente posible para prevenir incidentes de seguridad de la información. El mecanismo de reporte debería ser sencillo, accesible, y disponible según sea posible. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

Información adicional

Los empleados, los contratistas y los usuarios de terceros deberían ser aconsejados de no procurar probar debilidades sospechadas de seguridad. Pruebas de debilidades pueden ser interpretadas como un potencial uso erróneo del sistema y podrían también causar daño al sistema de información o al servicio y resultar en una responsabilidad legal para el individuo que realizaba la prueba.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

OBJETIVO: Asegurar que un enfoque constante y eficaz se aplica a la gestión de los incidentes de seguridad de la información. Deberían establecerse responsabilidades y procedimientos para manejar eventos y debilidades de seguridad de la información con eficacia una vez que se hayan reportado. Un proceso de mejora continua debería aplicarse a la respuesta para la supervisión, evaluación, y gestión general de incidentes de seguridad de la información. Cuando se requiera evidencia, la misma debería ser recogida asegurando conformidad con requisitos legales.

13.2.1 Responsabilidades y procedimientos

Control

Deberían establecerse las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de seguridad de la información.

Guía de implementación

Además del reporte de los eventos y de las debilidades de seguridad de la información (véase también el apartado 13.1), la supervisión de sistemas, alarmas, y vulnerabilidades (10.10.2) debería utilizarse para detectar incidentes de seguridad de la información. Las siguientes recomendaciones para procedimientos de gestión de incidentes de seguridad de la información deberían ser consideradas:

a) deberían establecerse procedimientos para manejar diversos tipos de incidente de seguridad de la información, incluyendo:

1) fallos del sistema de información y pérdida de servicio;
2) código malicioso (véase el apartado 10.4.1);
3) negación de servicio;

4) errores producidos por datos de negocio incompletos o inexactos;
5) violaciones de la confidencialidad e integridad;
6) uso erróneo de los sistemas de información;

b) además de planes de contingencia normales (véase el apartado 14.1.3), los procedimientos deberían también cubrir (véase también el apartado 13.2.2):

1) análisis e identificación de la causa del incidente;
2) contención;
3) la planificación e implementación de la acción correctiva para prevenir la repetición, en caso de necesidad;
4) comunicación con aquellos afectados por o implicados en la recuperación del incidente;
5) reporte del evento a la autoridad apropiada;

c) pistas de auditoría y evidencia similar deberían recogerse (véase el apartado 13.2.3) y asegurarse, como sea apropiado, para:

1) análisis interno del problema;
2) uso como evidencia forense en lo referente a una violación potencial de un contrato o de un requisito regulador o en la eventualidad de procesos civiles o criminales, por ejemplo, bajo legislación de abuso de sistemas o de protección de los datos;
3) negociar una compensación por parte de proveedores de software y de servicio;

d) la acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada; los procedimientos deberían asegurar que:

1) solamente al personal claramente identificado y autorizado se le permite el acceso a los sistemas en producción y a sus datos (véase también el apartado 6.2 para el acceso externo);
2) todas las medidas de urgencia tomadas se documentan detalladamente;
3) las medidas de urgencia se reportan a la dirección y se repasan de una manera ordenada;
4) la integridad de los sistemas y de los controles del negocio se confirma con un retraso mínimo.

Los objetivos para la gestión de incidentes de seguridad de la información se deberían acordar con la dirección, y debería asegurarse que aquellos responsables de esta gestión entienden las prioridades de la organización para manejar incidentes de seguridad de la información.

Información adicional

Los incidentes de seguridad de la información pueden superar los límites de la organización y los nacionales. Para responder a tales incidentes existe una necesidad en aumento de coordinar respuesta y compartir la información sobre estos incidentes con organizaciones externas como sea apropiado.

13.2.2 Aprendiendo de los incidentes de seguridad de la información

Control

Deberían existir mecanismos establecidos para permitir que los tipos, volúmenes y costos de los incidentes de seguridad de la información sean cuantificados y supervisados.

Guía de implementación

La información obtenida de la evaluación de incidentes de seguridad de la información debería ser usada para identificar incidentes recurrentes o de alto impacto.

Información adicional

La evaluación de incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de futuras ocurrencias, o para ser tomada en cuenta en el proceso de revisión de la política de seguridad (véase el apartado 5.1.2).

13.2.3 Recolección de evidencia

Control

Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de la información, implica una acción legal (civil o criminal), se debería recolectar, retener y presentar evidencia para cumplir con las reglas de presentación de evidencia en la(s) jurisdicción(es) relevante(s).

Guía de implementación

Deberían desarrollarse y seguirse procedimientos internos al recoger y presentar la evidencia para los propósitos de acción disciplinaria manejados dentro de una organización.

En general, las reglas para manejo de evidencias cubren:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte;

b) peso de evidencia: la calidad y lo completitud de la evidencia.

Para alcanzar la admisibilidad de la evidencia, la organización debería asegurarse de que sus sistemas de información cumplen con cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia proporcionado debería estar de acuerdo con cualquier requisito aplicable. Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante una pista sólida de la evidencia. En general, dicha pista sólida se puede establecer bajo las siguientes condiciones:

a) para los documentos en papel: el original se guarda de manera segura con un registro del individuo que encontró el documento, dónde fue encontrado el documento, cuándo el documento fue encontrado y quién fue testigo del descubrimiento; cualquier investigación debería asegurarse de que las originales no sean alterados;

b) para la información sobre medios de computadora: las imágenes o las copias espejo (dependiendo de requisitos aplicables) de cualquier medio removible, información en discos duros o en memoria deberían ser tomadas para asegurar su disponibilidad; el registro de todas las acciones durante el proceso de copiado debería guardarse y el proceso debería efectuarse ante testigos; los medios originales y el registro (si este no es posible, por lo menos una imagen espejo o copia) deberían guardarse de manera segura e intactos.

Cualquier trabajo forense debería realizarse solamente sobre copias del material de evidencia. La integridad de todo el material de evidencia debería ser protegida. La copia de material de evidencia debería supervisarse por personal digno de confianza y debería registrarse información sobre cuándo y dónde el proceso de copiado fue ejecutado, quién realizó las actividades de copiado y qué herramientas y programas se han utilizado.

Información adicional

Cuando un acontecimiento de seguridad de la información se detecta por primera vez, puede no ser obvio si el acontecimiento dará lugar a una acción legal o no. Por lo tanto, existe el peligro que evidencia necesaria

sea destruida intencionalmente o accidentalmente antes que la seriedad del incidente se observe. Es recomendable implicar a un abogado o a la policía temprano en cualquier demanda legal contemplada y asesorarse sobre la evidencia requerida.

La evidencia puede superar límites de la organización y/o jurisdiccionales. En tales casos, se debería asegurar que la organización tiene derecho a recoger la información requerida como evidencia. Los requisitos de diversas jurisdicciones deberían también considerarse para maximizar la posibilidad de admisión de la misma a través de las jurisdicciones relevantes.

14 Gestión de la continuidad del negocio

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

OBJETIVO: Contrarrestar interrupciones a las actividades del negocio y proteger los procesos críticos del negocio contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su restauración oportuna.

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio se deberían someter a un análisis del impacto en el negocio. Se deberían desarrollar e implementar planes de continuidad del negocio para garantizar la restauración oportuna de las operaciones esenciales. La seguridad de la información debería ser una parte integral de todo el proceso de continuidad del negocio y de otros procesos de gestión en la organización.

La gestión de la continuidad del negocio debería incluir controles para la identificación y reducción de riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para los procesos del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Guía de implementación

El proceso debería reunir los siguientes elementos clave para la gestión de la continuidad del negocio:

a) comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio (véase el apartado 14.1.2);

b) identificación de todos los activos involucrados en los procesos críticos del negocio (véase el apartado 7.1.1);
c) comprensión del impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información (es importante encontrar soluciones para manejar los incidentes que producen impactos

menores, así como los incidentes graves que puedan amenazar la viabilidad de la organización), y establecer los objetivos del negocio para los servicios de procesamiento de información;

d) consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos;

e) identificación y consideración de la implementación de controles preventivos y mitigantes adicionales;

f) identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información;

g) garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización;

h) formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada de continuidad del negocio (véase el apartado 14.1.3);

i) prueba y actualización regular de los planes y procesos establecidos (véase el apartado 14.1.5);

j) garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización (véase el apartado 6.1.1).

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

Guía de implementación

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo, fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y período de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Control

Se deberían desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requeridos, después de la interrupción o la falla de los procesos críticos para el negocio.

Guía de implementación

En el proceso de planificación de la continuidad del negocio se deberían considerar los siguientes aspectos:

a) identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio;

b) identificar la pérdida aceptable de información y servicios;

c) implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas; es necesario atender la evaluación de las dependencias internas y externas del negocio y de los contratos establecidos;

d) procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración;

e) documentación de procedimientos y procesos acordados;

f) formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis;

g) pruebas y actualización de los planes.

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo, la restauración de servicios de comunicación específicos para los clientes en un lapso de tiempo aceptable. Los servicios y recursos que lo facilitan deberían identificarse, incluyendo el personal, los recursos no relacionados con el procesamiento de información, al igual que las disposiciones de respaldo para los servicios de procesamiento de información. Estas disposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdos recíprocos o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organización y, por lo tanto, pueden contener información sensible que es necesario proteger adecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenar en un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre en la sede principal. La dirección debería garantizar que las copias de los planes de continuidad del negocio están actualizadas y protegidas con el mismo nivel de seguridad que se aplica en la sede principal. De igual modo, el otro material necesario para ejecutar los planes de continuidad se debería almacenar en un sitio lejano.

Si se utilizan lugares alternos temporales, el nivel de los controles de seguridad implementados en estos lugares debería ser equivalente al de la sede principal.

Información adicional

Es conveniente observar que los planes y las actividades de la gestión de crisis (véase el apartado 14.1.3.f)) pueden ser diferentes de la gestión de la continuidad del negocio; es decir, se puede presentar una crisis que se pueda adaptar con procedimientos de gestión normales.

14.1.4 Estructura para la planificación de la continuidad del negocio

Control

Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y tratar de forma consistente los requisitos de la seguridad de la información, así como identificar las prioridades para pruebas y mantenimiento.

Guía de implementación

Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo, el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del pan. Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo, planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un dueño específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los dueños de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de seguridad de la información identificados y considera los siguientes aspectos:

a) las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan;

b) los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio;

c) los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos;

d) los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración;

e) los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad;

f) una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan;

g) actividades de concientización, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces;

h) las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes;

i) los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

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

Control

Los planes de continuidad del negocio se deberían someter a pruebas y actualizar regularmente para asegurar su actualización y su eficacia.

Guía de implementación

Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, y conocen su función cuando se ejecuta un plan.

La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionarán en condiciones reales. Éstas incluirían:

a) la prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones);

b) las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes);

c) las pruebas de recuperación técnica (garantizando que los sistemas de información se pueden restaurar eficazmente);

d) las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal);

e) las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído);

f) los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Éstas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se deberían registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidad para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se reflejan en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, la mejora de los sistemas y cambios en:

a) el personal;

b) las direcciones o los números telefónicos;

c) la estrategia del negocio;

d) los lugares, dispositivos y recursos;

e) la legislación;

f) los contratistas, proveedores y clientes principales;

g) los procesos existentes, nuevos o retirados;

h) los riesgos (operativos y financieros).

15 Cumplimiento

15.1 Cumplimiento de los requisitos legales

OBJETIVO: Evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual, y de cualquier requisito de seguridad.

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

Debería buscarse asesoramiento sobre requisitos legales específicos de los asesores jurídicos de la organización, o de profesionales del derecho cualificados. Los requisitos legales varían de un país a otro y pueden variar para la información creada en un país y que se transmite a otro (es decir, el flujo de datos transfronterizo).

15.1.1 Identificación de la legislación aplicable.

Control

Todos los requisitos estatutarios, reguladores, y contractuales relevantes y el enfoque de la organización para cumplir estos requisitos deberían ser definidos explícitamente, documentados, y mantenidos al día para cada sistema de información y para la organización.

Guía de implementación

Los controles específicos y responsabilidades individuales para cumplir con los requisitos anteriores deberían ser definidos y documentados de manera similar.

15.1.2 Derechos de propiedad intelectual (IPR)

Control

Deberían implementarse los procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reguladores y contractuales sobre el uso del material protegido por derechos de propiedad intelectual, y sobre el uso de los productos de software propietario.
Guía de implementación

Deberían considerarse las siguientes recomendaciones para proteger cualquier material que pueda ser considerado propiedad intelectual:

a) publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal de los productos de software e información;

b) adquirir software sólo de fuentes conocidas y de buena reputación, para asegurar que los derechos de copia del software no han sido violados;

c) mantener la concientización sobre los derechos de copia del software y la política de adquisiciones, publicando la intención de adoptar medidas disciplinarias para el personal que los viole;

d) mantener un registro apropiado de activos, e identificar todos aquellos protegido por derecho de propiedad intelectual;

e) mantener los documentos que acrediten la propiedad de licencias, discos originales, manuales, etc.;

f) implantar controles para asegurar que no se sobrepasa el número máximo de usuarios permitidos;

g) comprobar que sólo se instala software autorizado y productos bajo licencia;

h) establecer una política de mantenimiento de las condiciones adecuadas de licencia;

i) establecer una política de eliminación de software o de su transferencia a terceros;

j) usar herramientas adecuadas de auditoría;

k) cumplir con los términos y condiciones de uso del software y de la información obtenidos de redes públicas;

l) no duplicar, ni convertir a otro formato o extraer información de las grabaciones comerciales (película, audio) con excepción de lo permitido por los derechos de copia;

m) no copiar total o parcialmente, libros, artículos, informes u otros documentos, con excepción de lo permitido por los derechos de copia.

Información adicional

Los derechos de propiedad intelectual incluyen software o documentos con derecho de copia, derechos de diseño, marcas registradas, patentes y código fuente licenciado.

Los productos de software propietario se suelen entregar con un contrato de licencia que especifica términos y condiciones del licenciamiento, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar la generación de copias únicamente a finalidades de respaldo. La situación para el software desarrollado por la organización en materia de derechos de propiedad intelectual debería ser clarificada con el personal.

Los requisitos legales, normativos y contractuales pueden plantear restricciones a la copia de material propietario. En particular pueden requerir que sólo pueda utilizarse material desarrollado por la organización o bien proporcionado por el proveedor y bajo su licencia para la organización. La infracción de derechos de copia puede conducir a acciones legales que impliquen procedimientos judiciales.

15.1.3 Protección de los registros de la organización

Control

Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en acuerdo con los requisitos estatutarios, reguladores, contractuales y del negocio.

Guía de implementación

Los registros se deberían categorizar según el tipo, como por ejemplo: registros contables, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno de los cuales con los detalles de plazos de retención y medios de almacenamiento como papel, microfichas, medios magnéticos u ópticos).

Cualquier material relacionado con claves criptográficas y programas asociados con archivos cifrados o firmas digitales (véase el apartado 12.3), se debería guardar para permitir el descifrado de los registros durante el tiempo que los mismos son retenidos.

Se debería considerar la posibilidad de deterioro de los medios utilizados para almacenar los registros. Se deberían implantar procedimientos para su almacenamiento y utilización de acuerdo con las recomendaciones del fabricante. Para el almacenamiento de larga duración, el uso del papel y la microficha deberían ser considerados.

Donde se utilicen medios de almacenamiento electrónico, se deberían incluir procedimientos para asegurar la habilidad para acceder a los datos (tanto al medio como a la lectura de los formatos en sí) a través de todo el período de retención, para salvaguardarlos contra su pérdida debida a un cambio futuro de tecnología.

Se deberían elegir los sistemas de almacenamiento tal que los datos requeridos puedan recuperarse de manera aceptable en tiempo y forma, dependiendo de los requisitos a satisfacer.

El sistema de almacenamiento y utilización debería asegurar una identificación clara de los registros y de su periodo de retención según lo definido por la legislación o las regulaciones nacionales o regionales, si es aplicable. Este debería permitir la destrucción apropiada de los registros tras dicho período cuando ya no los necesite la organización.

Para alcanzar los objetivos de salvaguardar los registros, se deberían tomar las siguientes medidas dentro de una organización:

a) deberían publicarse directrices sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información;

b) debería establecerse un calendario de retenciones que identifique los tipos esenciales de registros y los períodos de tiempo que deberían retenerse;

c) debería mantenerse un inventario de las fuentes de información clave;

d) deberían implantarse los controles y medidas apropiados para la protección de los registros y la información contra su pérdida, destrucción o falsificación.

Información adicional

Algunos registros podrían requerir ser almacenados de manera segura tanto para cumplir con requisitos estatutarios, reguladores o contractuales, como para soportar actividades esenciales del negocio. Por ejemplo, los registros que puedan requerirse para acreditar que la organización opera dentro de las reglas estatutarias o reguladoras, para asegurar una defensa adecuada contra una posible acción civil o penal, o bien para confirmar el estado financiero de la organización respecto a los accionistas, partes externas y auditores. La legislación nacional u otras regulaciones podrían establecer el plazo y contenido de la información a retener.

Información adicional sobre la gestión de registros de una organización se puede encontrar en la norma ISO 15489-1.

15.1.4 Protección de los datos y privacidad de la información personal

Control

Debería asegurarse la protección y la privacidad de los datos, de acuerdo con la legislación y las regulaciones pertinentes, y si es aplicable, con las cláusulas contractuales.

Guía de implementación

Una política de protección y de privacidad de los datos de la organización debería ser desarrollada e implementada. Esta política se debería comunicar a todas las personas implicadas en el procesamiento de información personal.

El cumplimiento de esta política y de toda la legislación y regulaciones relevantes a la protección de los datos requiere una apropiada estructura de gestión y control. Este objetivo suele alcanzarse con mayor facilidad designando una persona responsable, por ejemplo un oficial de protección de datos, que oriente a los directores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos que deberían seguirse. La responsabilidad de manejar la información personal y de asegurar el conocimiento de los principios de la protección de los datos se debería establecer de acuerdo con la legislación y las regulaciones relevantes. Se deberían implementar medidas técnicas y organizacionales apropiadas para proteger la información personal.

Información adicional

Cierto número de países han introducido legislación colocando controles en la recolección, el procesamiento y transmisión de datos personales (en general información de personas vivas que pueden ser identificadas a raíz de dicha información). Dependiendo de la respectiva legislación nacional, estos controles pueden imponer obligaciones a quien recoja, procese y transmita información personal, y pueden restringir la posibilidad de transferir estos datos a otros países.

15.1.5 Prevención del uso inadecuado de las instalaciones de procesamiento de la información

Control

Los usuarios deberían ser disuadidos de usar las instalaciones de procesamiento de la información para propósitos no autorizados.

Guía de implementación

La dirección debería aprobar el uso de instalaciones de procesamiento de la información. Cualquier uso de estas instalaciones para propósitos ajenos al negocio o no autorizados, sin la aprobación de la dirección (véase el apartado 6.1.4), debería ser visto como uso impropio de los recursos. Si cualquier actividad no autorizada se identifica mediante supervisión u otros medios, se debería poner en conocimiento del director responsable para la consideración de la acción disciplinaria y/o legal apropiada.

Debería solicitarse asesoría legal antes de la implantación de procedimientos de supervisión.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y de los lugares que son supervisados para detectar usos no autorizados. Esto puede conseguirse mediante la entrega a los usuarios de una autorización escrita cuya copia debería firmar el usuario y ser retenida en forma segura por parte de la organización. Debería informarse a los empleados de la organización, a los contratistas y a los usuarios de terceras partes que no se permitirá otro acceso que no sea el autorizado.

Al conectarse (*log-on*) en su puesto de trabajo, un mensaje de advertencia debería indicar en la pantalla que el sistema al que se entra es privado y que no se permite el acceso no autorizado. El usuario tiene que darse

por enterado y reaccionar de forma apropiada al mensaje para poder continuar el proceso de conexión (véase el apartado 11.5.1).

Información adicional

Las instalaciones de procesamiento de la información de una organización son consideradas principalmente o exclusivamente para los propósitos del negocio. La detección de intrusos, la inspección de contenidos, y otras herramientas de supervisión pueden ayudar a prevenir y a detectar el uso inadecuado de las instalaciones de procesamiento de la información.

Muchos países ya tienen legislación de protección contra el mal uso de los recursos informáticos. El uso de los mismos con fines no autorizados puede constituir un delito penal.

La legalidad de la supervisión y el control del uso de los recursos varían de un país a otro y puede requerir que se avise de su existencia a los empleados y/o que se requiera su consentimiento. Cuando el sistema que es accedido se utiliza para el acceso público (por ejemplo, un servidor Web público) y está sujeto a supervisiones de seguridad, un mensaje debería ser exhibido advirtiendo esto.

15.1.6 Regulación de los controles criptográficos

Control

Deberían utilizarse controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones relevantes.

Guía de implementación

Los siguientes puntos deberían considerarse para el cumplimiento de los acuerdos, las leyes, y las regulaciones relevantes:

a) restricciones en la importación y/o en la exportación de hardware y de software para realizar funciones criptográficas;

b) restricciones en la importación y/o en la exportación de hardware y de software que se diseña para tener funciones criptográficas incluidas en él;

c) restricciones en el uso de cifrado;

d) métodos obligatorios o fijados a discreción de acceso por parte de las autoridades de los países a la información cifrada mediante hardware o software para proporcionar la confidencialidad del contenido.

Mediante el asesoramiento jurídico se debería intentar asegurar el cumplimiento de leyes y regulaciones nacionales. Antes que información cifrada o controles criptográficos sean trasladados a otro país, también debería tenerse en cuenta el asesoramiento jurídico.

15.2 Cumplimiento de la política y las normas de seguridad, y cumplimiento técnico.

OBJETIVO: Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.

La seguridad de los sistemas de información debería ser revisada regularmente. Tales revisiones se deberían realizar contra las políticas de seguridad y las plataformas técnicas apropiadas, los sistemas de información se deberían auditar para cumplir con normas aplicables de implantación de la seguridad y controles documentados de la seguridad.

15.2.1 Cumplimiento de las políticas y normas de seguridad.

Control

Los directores deberían asegurarse que se cumplen correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para lograr el cumplimiento de políticas y normas de seguridad.

Guía de implementación

Los directores deberían revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas de seguridad apropiadas, las normas, y cualquier otro requisito de seguridad.

Si algún incumplimiento se encuentra como resultado de la revisión, los directores deberían:

a) determinar las causas del incumplimiento;

b) evaluar la necesidad de acciones para asegurar que no se repita el incumplimiento;

c) determinar e implementar las acciones correctivas apropiadas;

d) revisar la acción correctiva tomada.

Los resultados de las revisiones y de las acciones correctivas realizadas por los directores deberían ser registrados y estos expedientes deberían ser mantenidos. Los directores deberían reportar los resultados a las personas que realizan las revisiones independientes (véase el apartado 6.1.8), cuando la revisión independiente se realice en el área de su responsabilidad.

Información adicional

El seguimiento operacional del uso del sistema se cubre en el apartado 10.10.

15.2.2 Verificación del cumplimiento técnico

Control

Los sistemas de información deberían ser revisados regularmente para verificar el cumplimiento con las normas de implementación de la seguridad.

Guía de implementación

La verificación del cumplimiento técnico debería realizarse manualmente por un ingeniero de sistemas experimentado (con apoyo de herramientas de software apropiadas si es necesario), y/o con la ayuda de herramientas automatizadas que generen un informe técnico para su posterior interpretación por parte de un especialista técnico.

Si se utilizan pruebas de intrusión o evaluaciones de vulnerabilidad, se debería tener cuidado pues estas actividades podrían comprometer la seguridad del sistema. Tales pruebas deberían ser planificadas, documentadas y repetibles.

Cualquier verificación del cumplimiento técnico debería realizarse solamente por las personas competentes, autorizadas, o bajo supervisión de tales personas.

Información adicional

La verificación del cumplimiento técnico comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de la conformidad requiere asistencia técnica especializada.

La verificación del cumplimiento también comprende, por ejemplo, pruebas de intrusión y evaluación de vulnerabilidades, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito. Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas.

Las pruebas de intrusión y la evaluación de vulnerabilidades proporcionan una muestra de un sistema en un estado y momento específico. La muestra se limita a esas porciones del sistema probado realmente durante el o los intentos de penetración. Las pruebas de intrusión y la evaluación de vulnerabilidades no son un sustituto para la evaluación de riesgo.

15.3 Consideraciones sobre la auditoría de sistemas de información

OBJETIVO: Maximizar la efectividad de, y reducir al mínimo la interferencia desde o hacia, el proceso de auditoría del sistema de información.

Se deberían establecer controles para salvaguardar los sistemas en producción y las herramientas de auditoría durante las auditorías del sistema de información.

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

15.3.1Controles de auditoría de sistemas de información

Control

Deberían planificarse cuidadosamente y acordarse los requisitos y actividades de auditoría que impliquen verificaciones en los sistemas en producción, para minimizar el riesgo de interrupción de los procesos de negocio.

Guía de implementación

Las siguientes recomendaciones deberían tenerse en cuenta:

a) deberían acordarse los requisitos de auditoría con la dirección apropiada;

b) debería acordarse y controlarse el alcance de las verificaciones;

c) las verificaciones se deberían limitar a accesos de sólo lectura al software y a los datos;

d) otro acceso distinto a solo lectura, solamente se debería permitir para copias aisladas de archivos del sistema, que se deberían borrar cuando se complete la auditoría, o bien brindar la adecuada protección si hay obligación de mantener tales archivos como requisito de documentación de la auditoría;

e) los recursos para realizar comprobaciones deberían ser explícitamente identificados y puestos a disposición;

f) los requisitos para procesos especiales o adicionales deberían ser identificados y acordados;

g) todo acceso se debería supervisar y registrar para producir un histórico para referencia; se debería considerar el uso de las pistas con impresión horaria (*timestamped*) en el histórico para los datos o los sistemas críticos;

h) todos los procedimientos, requisitos y responsabilidades deberían estar documentados;

i) la o las personas encargadas de la auditoría deberían ser independientes de las actividades auditadas.

15.3.2 Protección de las herramientas de auditoría de sistemas de información.

Control

Deberían protegerse los accesos a las herramientas de auditoría de sistemas de información para evitar cualquier posible mal uso o el compromiso de las mismas.

Guía de implementación

Las herramientas de auditoría de sistemas de información, por ejemplo, archivos de datos o software, deberían estar separadas de los sistemas en producción y de desarrollo y no se mantendrán en bibliotecas de cintas o en áreas de los usuarios, salvo que se les proporcione un nivel apropiado de protección adicional.

Información adicional

Si terceras partes están involucradas en una auditoría, pudo haber un riesgo de mal uso de las herramientas de auditoría, y de la información accedida por esta organización externa. Los controles tales como los descritos en 6.2.1 (identificar los riesgos) y en 9.1.2 (restringir el acceso físico) se pueden considerar para tratar este riesgo, debería ser tomada en cuenta cualquier consecuencia, como ser el cambio inmediato de contraseñas que hayan sido divulgadas a los auditores.

Bibliografía

[1] ISO/IEC Guide 2: 1996, Standardization and Related Activities - General Vocabulary.

[2] ISO/IEC Guide 73:2002, Risk Management - Vocabulary - Guidance for Use in Standards.

[3] ISO/IEC 13335-1:2004, Information Technology - Security Techniques - Management of Information and Communications Technology Security - Part 1: Concepts and Models for Information and Communications Technology Security Management.

[4] ISO/IEC TR 13335-3:1998, Information Technology Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT security.

[5] ISO/IEC 13888-1:1997, Information Technology - Security Techniques - Non-repudiation - Part 1: General.

[6] ISO/IEC 11770-1:1996, Information Technology - Security Techniques - Key Management - Part 1: Framework.

[7] ISO/IEC 9796-2:2002, Information Technology - Security techniques - Digital Signatures Schemes Giving Message Recovery - Part 2: Integer Factorization Based Mechanisms.

[8] ISO/IEC 9796-3:2000, Information Technology - Security Techniques - Digital Signatures Schemes Giving Message Recovery - Part 3: Discrete Logarithm Based Mechanisms.

[9] ISO/IEC 14888-1:1998, Information technology - Security Techniques - Digital Signatures with Appendix - Part 1: General.

[10] ISO/IEC 15408-1:1999, Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introduction and General Model.

[11] ISO/IEC 14516:2002, Information Technology - Security Techniques - Guidelines for the use and Management of Trusted Third Party Services.

[12] ISO 15489-1:2001, Information and Documentation - Records Management - Part 1: General.

[13] ISO 10007:2003, Quality Management Systems - Guidelines for Configuration Management.

[14] ISO/IEC 12207:1995, Information Technology - Software Life Cycle Processes.

[15] ISO 19011:2002, Guidelines for Quality and/or Environmental Management System Auditing.

[16] OECD Guidelines for the Security of Information Systems and Networks: "Towards a Culture of Security", 2002.

[17] OECD Guidelines for Cryptography Policy, 1997.

[18] IEEE P1363-2000: Standard Specifications for Public-Key Cryptography.

[19] ISO/IEC 18028-4, Information Technology - Security Techniques - IT Network Security – Part 4: Securing Remote Access.

[20] ISO/IEC TR 18044, Information Technology - Security Techniques - Information Security Incident Management.