ESTÁNDAR INTERNACIONAL

ISO/IEC 17799

Segunda Edición
2005-06-15

Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información

Índice

Prefacio

ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos internacionales miembros de ISO e IEC participan en el desarrollo de Estándares Internacionales a través de los comités establecidos por la organización respectiva para lidiar con áreas particulares de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no-gubernamentales, junto con ISO e IEC, también participan en el trabajo. En el campo de la tecnología de la información. ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Los Estándares Internacionales son diseñados en concordancia con las reglas dadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Estándares Internacionales. Los anteproyectos de los Estándares Internacionales adoptados por el comité técnico son presentados a los organismos nacionales para su votación. La publicación de un Estándar Internacional requiere de la aprobación de por lo menos 75% de los organismos nacionales que emiten un voto.

Se presta atención a la posibilidad que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no debieran ser responsables de identificar todos o alguno de dichos de derechos de patente.

ISO/IEC 17799 fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Técnicas de seguridad TI*.

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

El ISO/IEC JTC 1/SC 27 viene desarrollando una familia de Estándares Internacionales para el Sistema de Gestión de Seguridad de la Información (ISMS). La familia incluye Estándares Internacionales sobre requerimientos gestión del riesgo, métrica y medición, y el lineamiento de implementación del sistema de gestión de seguridad de la información. La familia adoptará el esquema de numeración utilizando las series del número 27000 en secuencia.

A partir del 2007, se propone incorporar una edición nueva del ISO/IEC 17799 en este nuevo esquema de numeración con el nombre ISO/IEC 27002.

0 Introducción

0.1 ¿Qué es seguridad de la información?

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades (ver también los Lineamientos OECD de la Seguridad de Sistemas y Redes de Información).

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de

seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

0.2 ¿Por qué se necesita seguridad de la información?

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

0.3 ¿Cómo establecer los requerimientos de seguridad?

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

Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.
Otra fuente es el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

0.4 Evaluando los riesgos de la seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

Se puede encontrar más información de la evaluación de los riesgos de seguridad en la cláusula 4.1 “Evaluando los riesgos de la seguridad”.

0.5 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas conforme sea apropiado. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes.

Algunos de los controles en este estándar se pueden considerar principios guías para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Se

explican con mayor detalle más abajo bajo el título “Punto de inicio de la seguridad de la información”.

Se puede encontrar más información sobre la selección de controles y otras opciones de tratamiento del riesgo en la cláusula 4.2 “Tratamiento de los riesgos de seguridad”.

0.6 Punto de inicio de la seguridad de la información

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legislativos esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

a) protección de data y privacidad de la información personal (ver 15.1.4);
b) protección de los registros organizacionales (ver 15.1.3);
c) derechos de propiedad intelectual (ver 15.1.2).

Los controles considerados práctica común para la seguridad de la información incluyen:

a) documento de la política de seguridad de la información (ver 5.1.1);
b) asignación de responsabilidades de la seguridad de la información (ver 6.1.3);
c) conocimiento, educación y capacitación en seguridad de la información (ver 8.2.2);
d) procesamiento correcto en las aplicaciones (ver 12.2);
e) gestión de la vulnerabilidad técnica (ver 12.6);
f) gestión de la continuidad comercial (ver 14);
g) gestión de los incidentes y mejoras de la seguridad de la información (ver 13.2).

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en este estándar son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

0.7 Factores de éxito críticos

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

a) política, objetivos y actividades de seguridad de información que reflejan los objetivos comerciales;

b) un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;

c) soporte visible y compromiso de todos los niveles de gestión;

d) un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;

e) marketing efectivo de la seguridad de la información con todo los gerentes, empleados y otras partes para lograr conciencia sobre el tema;

f) distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los gerentes, empleados y otras partes involucradas;

g) provisión para el financiamiento de las actividades de gestión de la seguridad de la información;

h) proveer el conocimiento, capacitación y educación apropiados;

i) establecer un proceso de gestión de incidentes de seguridad de la información;

j) implementación de un sistema de medición[1] que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

0.8 Desarrollo de sus propios lineamientos

Este código de práctica puede ser visto como un punto de inicio para desarrollar los lineamientos específicos de la organización. No todos los controles y lineamientos en este código de práctica pueden ser aplicables. Es más, se pueden requerir controles y lineamientos adicionales no incluidos en este estándar. Cuando los documentos son desarrollados conteniendo lineamientos o controles adicionales, cuando sea aplicable podría ser útil incluir referencias cruzadas con las cláusulas en este estándar para facilitar el chequeo de conformidad realizado por los auditores y socios comerciales.

Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información

[1] Noten que las mediciones de la seguridad de la información están fuera del ámbito de este estándar.

1 Alcance

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo. Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

2 Términos y definiciones

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

2.1

Activo

Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004)

2.2

Control

Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

NOTA. El control también se utiliza como sinónimo de salvaguarda o contramedida.

2.3

Lineamiento

Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas (ISO/IEC 13335-1:2004)

2.4

Medios de procesamiento de la información

Cualquier sistema, servicio o infraestructura de procesamiento de la información, o los locales físicos que los alojan

2.5

Seguridad de la información

Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad

2.6

Evento de seguridad de la información

Cualquier evento de seguridad de la información es una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad. (ISO/IEC TR 18044:2004)

2.7

Incidente de seguridad de la información

Un incidente de seguridad de la información es indicado por un solo evento o una serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (ISO/IEC TR 18044:2004)

2.8

Política

Intención y dirección general expresada formalmente por la gerencia

2.9

Riesgo

Combinación de la probabilidad de un evento y su ocurrencia (ISO/IEC Guía 73:2002)

2.10

Análisis del riesgo

Uso sistemático de la información para identificar las fuentes y calcular el riesgo

2.11

Análisis del riesgo

Proceso general del análisis del riesgo y la evaluación del riesgo (ISO/IEC Guía 73: 2002)

2.12

Evaluación del riesgo

Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo (ISO/IEC Guía 73: 2002)

2.13

Gestión del riesgo

Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

NOTA. La gestión del riesgo normalmente incluye la evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. (ISO/IEC Guía 73: 2002)

2.14

Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo. (ISO/IEC Guía 73: 2002)

2.15

Tercera persona

Esa persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión. (ISO/IEC Guía 2: 1996)

2.16

Amenaza

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004)

2.17

Vulnerabilidad

La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas. (ISO/IEC 13335-1:2004)

3 Estructura de este estándar

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

3.1 Cláusulas

Cada cláusula contiene un número de categorías de seguridad principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de 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 Ambiental (2);
f) Gestión de Comunicaciones y Operaciones (10);
g) Control de Acceso (7);
h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6);
i) Gestión de Incidentes de Seguridad de la Información (2);
j) Gestión de la Continuidad Comercial (1);
k) Conformidad (3).

Nota: El orden de las cláusulas en este estándar no implica su importancia. Dependiendo de las circunstancias, todas las cláusulas pueden ser importantes; por lo tanto, cada organización que aplica este estándar debiera identificar las cláusulas aplicables, cuán importante son y su aplicación a los procesos comerciales individuales. También, las listas en este estándar no están por orden de prioridad a no ser que se así se especifique.

3.2 Categorías de seguridad principales

Cada categoría de seguridad contiene:

a) un objetivo de control que establece lo que se debiera lograr; y
b) uno o más controles que se pueden aplicar para lograr el objetivo de control.

Las descripciones del control están estructuradas de la siguiente manera:

Control

Define el enunciado de control específico para satisfacer el objetivo de control.

Lineamiento de implementación

Proporciona información más detallada para apoyar la implementación del control y cumplir con el objetivo de control. Parte de este lineamiento puede no ser adecuado en todos los casos y por lo tanto, pueden ser adecuadas otras maneras para implementar el control.

Otra información

Proporciona más información que tal vez se deba considerar, por ejemplo consideraciones legales y referencias a otros estándares.

4 Evaluación y tratamiento del riesgo

4.1 Evaluación de los riesgos de seguridad

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

El alcance de la evaluación del 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 es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Lineamientos para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad TI).

4.2 Tratamiento de los riesgos de seguridad

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicar los controles apropiados para reducir los riesgos;
b) aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;
c) evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;
d) transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

a) los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:
b) objetivos organizacionales;
c) requerimientos y restricciones operacionales;
d) costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;
e) la necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de

la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones. Como ejemplo, 10.1.3 describe cómo se pueden segregar las tareas para evitar el fraude y el error. En las organizaciones más pequeñas puede no ser posible segregar todas las tareas y pueden ser necesarias otras maneras para lograr el mismo objetivo de control. En otro ejemplo, 10.10 describe cómo se debiera monitorear el uso del sistema y recolectar la evidencia. Los controles descritos; por ejemplo, bitácora de eventos; podrían entrar en conflicto con la legislación aplicable, como la protección de la privacidad para los clientes o en el centro de trabajo.

Se debieran considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño. El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Se debiera tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que se debiera implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización.

5 Política de seguridad

5.1 Política de seguridad de la información

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.
La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

5.1.1 Documento de la política de seguridad de la información

Control

El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

Lineamiento de implementación

El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El documento de la política debiera contener enunciados relacionados con:

a) una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información (ver introducción);

b) un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales;

c) un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo;

d) una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo:

   1. conformidad con los requerimientos legislativos, reguladores y restrictivos,
   2. educación, capacitación y conocimiento de seguridad,
   3. gestión de la continuidad del negocio,
   4. consecuencias de las violaciones de la política de seguridad de la información;

e) una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información,

f) referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.

Esta política de seguridad de la información se debiera comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector objetivo.

Otra información

La política de seguridad de la información podría ser una parte del documento de política general. Si la política de seguridad de la información se distribuye fuera de la organización, se

debiera tener cuidado de no divulgar información confidencial. Se puede encontrar mayor información 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 debiera ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

Lineamiento de implementación

La política de la seguridad de la información debiera tener un dueño que tenga la responsabilidad gerencial aprobada para el desarrollo, revisión y evaluación de la política de seguridad. La revisión debiera incluir las oportunidades de evaluación para el mejoramiento de la política de seguridad de la información de la organización y el enfoque para manejar la seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias comerciales, condiciones legales o ambiente técnico.

La revisión de la política de seguridad de la información debiera tomar en cuenta los resultados de las revisiones de la gerencia. Debieran existir procedimientos de revisión gerencial, incluyendo un cronograma o el período de la revisión.

El input para la revisión gerencial debiera incluir información sobre:

a) retroalimentación de las partes interesadas;
b) resultados de revisiones independientes (ver 6.1.8);
c) estado de acciones preventivas y correctivas (ver 6.1.8 y 15.2.1);
d) resultados de revisiones gerenciales previas;
e) desempeño del proceso y conformidad con la política de seguridad de la información;
f) cambios que podrían afectar el enfoque de la organización en el manejo de la seguridad de la información, incluyendo los cambios en el ambiente organizacional; las circunstancias comerciales; la disponibilidad de recursos; condiciones contractuales, reguladoras y legales; o el ambiente técnico;
g) tendencias relacionadas con amenazas y vulnerabilidades;
h) incidentes de seguridad de información reportados (ver 13.1);
i) recomendaciones provistas por autoridades relevantes (ver 6.1.6).

Los outputs de la revisión gerencial debiera incluir cualquier decisión y acción relacionada con:

a) mejora del enfoque de la organización para manejar la seguridad de la información y sus procesos;
b) mejora de los objetivos de control y los controles;

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

Se debiera mantener un registro de la revisión gerencial. Se debiera obtener la aprobación de la gerencia para la política revisada.

6 Organización de la seguridad de la información

6.1 Organización interna

Objetivo: Manejar la seguridad de la información dentro de la organización. Se debiera establecer un marco referencial gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. La gerencia debiera aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la organización. Si fuese necesario, se debiera establecer una fuente de consultoría sobre seguridad de la información y debiera estar disponible dentro de la organización. Se debieran desarrollar contactos con los especialistas o grupos de seguridad externos, incluyendo las autoridades relevantes, para mantenerse actualizado con relación a las tendencias industriales, monitorear los estándares y evaluar los métodos y proporcionar vínculos adecuados para el manejo de los incidentes de seguridad de la información. Se debiera fomentar un enfoque multi-disciplinario para la seguridad de la información.

6.1.1 Compromiso de la gerencia con la seguridad de la información

Control

La gerencia debiera apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconociendo las responsabilidades de la seguridad de la información.

Lineamiento de implementación

La gerencia debiera:

a) asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén 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 de la información;

d) proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad;
e) proporcionar los recursos necesarios para la seguridad de la información;
f) aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización;
g) iniciar planes y programas para mantener la conciencia de seguridad de la información;
h) asegurar que la implementación de los controles de seguridad de la información sea coordinado en toda la organización.

La gerencia debiera identificar las necesidades de consultoría especializada interna o externa para la seguridad de la información, y revisar y coordinar los resultados de la consultoría a través de toda la organización.

Dependiendo del tamaño de la organización, estas responsabilidades podrían ser manejadas por un foro gerencial dedicado o por un organismo gerencial existente, como la junta de directores.

Otra información

Se encuentra mayor información en ISO/IEC 13335-1:2004.

6.1.2 Coordinación de la seguridad de la información

Control

Las actividades de la seguridad de la información debieran ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes.

Lineamiento de implementación

Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los gerentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Esta actividad debiera:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;
b) identificar cómo manejar las no-conformidades;

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

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

Si la organización no utiliza grupos inter-funcionales separados; por ejemplo, porque dicho grupo no es apropiado para el tamaño de la organización; las acciones arriba descritas debieran ser realizadas por otro organismo gerencial adecuado o un gerente individual.

6.1.3 Asignación de las responsabilidades de la seguridad de la información

Control

Todas las responsabilidades de la seguridad de la información debieran estar claramente definidas.

Lineamiento de implementación

La asignación de las responsabilidades de la seguridad de la información debiera realizarse en concordancia con la política de seguridad de la información (ver cláusula 4). Se debieran definir claramente las responsabilidades para la protección de los activos individuales y llevar a cabo los procesos de seguridad específicos. Cuando sea necesario, esta responsabilidad debiera ser complementada con un lineamiento más detallado para locales y medios de procesamiento de información específicos. Se debieran definir claramente las responsabilidades locales para la protección de activos y para llevar a cabo procesos de seguridad específicos, como la planeación de la continuidad del negocio.

Las personas con responsabilidades de seguridad asignadas pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo responsables y debieran determinar si cualquier tarea delegada ha sido realizada correctamente.

Se debieran establecer claramente las áreas de las cuales son responsables las diferentes personas; en particular se debiera realizar lo siguiente:

a) se debieran identificar y definir claramente los activos y procesos de seguridad asociados con cada sistema particular;
b) se debiera designar la entidad responsable de cada activo o proceso de seguridad y se debieran documentar los detalles de esta responsabilidad;
c) se debieran definir y documentar claramente los niveles de autorización.

Otra información

En muchas organizaciones se encargará a un gerente de seguridad de información para que asuma la responsabilidad general del desarrollo e implementación de la seguridad y fundamente la identificación de controles.

Sin embargo, la responsabilidad de asignar los recursos e implementar los controles con frecuencia permanece con los gerentes individuales. Una práctica común es nombrar a un propietario para cada activo quien entonces se vuelve responsable por su protección diaria.

6.1.4 Autorización de proceso para facilidades procesadoras de información.

Control

Un proceso de la gerencia para la autorización de facilidades nuevas de procesamiento de información, debiera ser definido e implementado.

Guía de implementación

Las siguientes guías debieran ser consideradas para el proceso de autorización:

a)Nuevas facilidades debieran tener apropiadas autorizaciones gerenciales para su autorización, autorizando su uso apropiado. La autorización también debe ser obtenida del gerente responsible por el ambiente del sistema de seguridad de información para asegurar que todas las políticas y requerimientos de seguridad relevantes son cumplidas.

b) Donde sea necesario, el hardware y el software debiera de ser chequeado para asegurar que son compatibles con otros componentes del sistema.

c) El uso de facilidades para el procesamiento de información, bien sean personales o privadas(ej: laptops, computadoras del hogar, sistemas hand-held) pueden introducir nuevas vulnerabilidades y controles necesarios debieran ser identificados e implementados.

6.1.5 Acuerdos de confidencialidad

Control

Se debieran identificar y revisar regularmente que los requerimientos de confidencialidad o acuerdos de no-divulgación reflejan las necesidades de la organización para proteger la información.

Lineamiento de implementación

Los acuerdos de confidencialidad o no-divulgación debieran tener en cuenta el requerimiento de proteger la información confidencial utilizando términos legalmente ejecutables. Para identificar los requerimientos de los acuerdos de confidencialidad o no-divulgación, se debieran considerar los siguientes elementos:

a) una definición de la información a protegerse (por ejemplo, información confidencial);
b) duración esperada de un acuerdo, incluyendo casos donde se podría necesitar mantener la confidencialidad indefinidamente;
c) acciones requeridas cuando se termina un acuerdo;
d) responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada (tal como "sólo lo que necesita saber");
e) propiedad de la información, secretos comerciales y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial;
f) uso permitido de la información confidencial, y los derechos del firmante para utilizar la información;
g) proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial;
h) condiciones para el retorno o destrucción de la información una vez que se termina el acuerdo; y
i) acciones esperadas a realizarse en caso de incumplimiento de este acuerdo.

En base a los requerimientos de seguridad de la organización, pueden ser necesarios otros elementos en los acuerdos de confidencialidad o no-divulgación.

Los acuerdos de confidencialidad y no-divulgación debieran cumplir con todas las leyes y regulaciones aplicables para la jurisdicción en la cual se aplica (ver también 15.1.1).

Los requerimientos de los acuerdos de confidencialidad o no-divulgación se debieran revisar periódicamente y cuando ocurren cambios que influyen en estos requerimientos.

Otra información

Los acuerdos de confidencialidad y no-divulgación protegen la información organizacional e informan a los firmantes de su responsabilidad de proteger, usar y divulgar información de una manera responsable y autorizada.

Puede existir la necesidad que una organización utilice formas diferentes de acuerdos de confidencialidad o no-divulgación en diferentes circunstancias.

6.1.6 Contacto con las autoridades

Control

Se debieran mantener los contactos apropiados con las autoridades relevantes.

Lineamiento de implementación

Las organizaciones debieran contar con procedimientos que especifiquen cuándo y cuáles autoridades (por ejemplo, policía, departamento de bomberos, autoridades supervisoras) contactar, y cómo se debieran reportar los incidentes de seguridad de la información identificados de una manera oportuna si se sospecha que se han incumplido las leyes.

Las organizaciones atacadas desde le Internet pueden necesitar que terceras personas externas (por ejemplo, un proveedor del servicio de Internet o un operador de telecomunicaciones) tome alguna acción contra la fuente de ataque.

Otra información

Mantener estos contactos puede ser un requerimiento para apoyar el manejo de un incidente de seguridad (Sección 13.2) o la continuidad del negocio y el proceso de planeación de contingencia (Sección 14). Los contactos con organismos reguladores también son útiles para anticipar y prepararse para cambios en la ley o las regulaciones que la organización debiera cumplir. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad; por ejemplo, departamento de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (en conexión con el routing de la línea) y los proveedores de agua (en conexión con los medios de enfriamientos del equipo).

6.1.7 Contacto con grupos de interés especial

Control

Se debieran mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

Lineamiento de implementación

Se debiera considerar la membresía en grupos de interés especial como un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad relevantes;
b) asegurar el entendimiento del ambiente de seguridad de la información sea actualizado y completo;

c) recibir advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades;
d) obtener acceso a consultoría especializada de seguridad de la información;
e) compartir e intercambiar información sobre tecnologías, productos, amenazas o vulnerabilidades;
f) proporcionar vínculos adecuados cuando se trata incidentes de seguridad de la información (ver también 13.2.1).

Otra información

Se pueden establecer acuerdos de intercambio de información para mejorar la cooperación y coordinación de temas de seguridad. Tales acuerdos debieran identificar los requerimientos de protección de información sensible.

6.1.8 Revisión independiente de la seguridad de la información

Control

Se debiera revisar el enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) de manera independiente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.

Lineamiento de implementación

La gerencia debiera iniciar la revisión independiente. Esta revisión independiente es necesaria para asegurar la continua idoneidad, eficiencia y efectividad del enfoque de la organización para manejar la seguridad de la información. La revisión debiera incluir las oportunidades de evaluación para el mejoramiento y la necesidad de cambios en el enfoque por seguridad, incluyendo políticas y objetivos de control.

Esta revisión debiera ser llevada a cabo por personas independientes al área de revisión; por ejemplo, la función de la auditoria interna, un gerente independiente o una tercera organización especializada en revisiones. Las personas que llevan a cabo estas revisiones debieran tener la capacidad y experiencia apropiada.

Los resultados de la revisión independiente se debieran registrar y reportar a la gerencia que inició la revisión. Se debieran mantener estos registros.

Si la revisión independiente identifica que el enfoque y la implementación de la organización para manejar la seguridad de la información no son adecuadas o no cumplen con la dirección para la seguridad de la información establecida en el documento de la política de seguridad de la información (ver 5.1.1), la gerencia debiera considerar acciones correctivas.

Otra información

El área, que los gerentes revisan regularmente (ver 15.2.1), también puede ser revisada independientemente. Las técnicas de revisión pueden incluir entrevistas, la gerencia revisando registros o revisando los documentos de la política de seguridad. ISO 19011:2002, Lineamientos para la calidad y/o auditoría de sistemas de gestión ambiental, también puede ser un lineamiento útil para llevar a cabo revisiones independientes, incluyendo el establecer e implementar un programa de revisión. La Sección 15.3 especifica los controles relevantes para la revisión independiente de un sistema de información operacional y el uso de las herramientas de auditoría del sistema.

6.2 Grupos o personas externas

Objetivo: Mantener la seguridad de la información y los medios de procesamiento de información de la organización que son ingresados, procesados, comunicados a, o manejados por, grupos externos.
La seguridad de la información y los medios de procesamiento de la información de la organización no debieran ser reducidos por la introducción de productos y servicios de grupos externos.
Se debiera controlar cualquier acceso a los medios de procesamiento de información de la organización y el procesamiento y comunicación de la información realizado por grupos externos.
Cuando existe la necesidad comercial de trabajar con grupos externos que pueden requerir acceso a la información y a los medios de procesamiento de información de la organización, u obtener o proveer un producto y servicio de o a un grupo externo, se debiera llevar a cabo una evaluación del riesgo para determinar las implicancias en la seguridad y los requerimientos de control. Se debieran acordar y definir los controles en un acuerdo con el grupo externo.

6.2.1 Identificación de los riesgos relacionados con los grupos externos

Control

Se debieran identificar los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se debieran implementar controles apropiados antes de otorgarles acceso.

Lineamiento de implementación

Donde existe la necesidad de permitir que un grupo externo tenga acceso a los medios de procesamiento de la información o la información de una organización, se debiera llevar a cabo una evaluación del riesgo (ver también Sección 4) para identificar cualquier requerimiento de controles específicos. La identificación de los riesgos relacionados con el acceso del grupo externo toma en cuenta los siguientes puntos:

a) los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo;
b) el tipo de acceso que tendrá el grupo externo a la información y los medios de procesamiento de la información; por ejemplo;
    1) acceso físico; por ejemplo, oficinas, edificios de cómputo, archivadores;
    2) acceso lógico; por ejemplo, a las bases de datos o sistemas de información de la organización;
    3) conectividad de red entre las redes de la organización y el grupo externo; por ejemplo, conexión permanente, acceso remoto;
    4) si el acceso se da fuera o dentro del local;
c) el valor y sensibilidad de la información involucrada, y su grado crítico para las operaciones comerciales;
d) los controles necesarios para proteger la información que no está destinada a ser accesible para los grupos externos;
e) el personal del grupo externo involucrado en el manejo de la información de la organización;
f) cómo se puede identificar a la organización y el personal autorizado que tiene acceso, cómo verificar la autorización, y con cuánta frecuencia se necesita reconfirmar esto;
g) los diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información;
h) el impacto del acceso no disponible para el grupo externo cuando lo requiere, y el grupo externo que ingresa o recibe información inexacta o confusa;
i) prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información y los daños potenciales, y los términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información;

j) requerimientos legales y reguladores y otras obligaciones contractuales relevantes que se debieran tomar en cuenta para el grupo externo;
k) cómo los intereses de cualquier parte interesada pueden verse afectados por los arreglos.

No se debiera otorgar acceso a los grupos externos a la información de la organización hasta que se hayan implementado los controles apropiados y, cuando sea factible, se haya firmado un contrato definiendo los términos y condiciones para la conexión o acceso y el contrato de trabajo. Generalmente, todos los requerimientos de seguridad resultantes del trabajo con grupos externos o controles internos se debieran reflejar en el acuerdo con el grupo externo (ver también 6.2.2 y 6.2.3).

Se debiera asegurar que el grupo externo esté al tanto de sus obligaciones y acepte las responsabilidades involucradas en tener acceso, procesar, comunicar o manejar la información y los medios de procesamiento de información de la organización.

Otra información

La información podría ser puesta en riesgo por grupos externos con una inadecuada gestión de seguridad. Se debieran identificar y aplicar controles para administrar el acceso del grupo externo a los medios de procesamiento de la información. Por ejemplo, si existe la necesidad especial de confidencialidad de la información, se podrían utilizar acuerdos de no-divulgación.

Las organizaciones pueden enfrentar riesgos asociados con procesos, gestión y comunicación inter-organizacional si se aplica un alto grado de abastecimiento externo, o cuando existen varios grupos externos involucrados.

Los controles 6.2.2 y 6.2.3 abarcan diferentes acuerdos con grupos externos; por ejemplo, incluyendo:

a) proveedores de servicio; tal como ISPs, proveedores de redes, servicios telefónicos, servicios de mantenimiento y soporte;
b) servicios de seguridad manejados;
c) clientes;
d) abastecimiento externo de medios y/o operaciones; por ejemplo, sistemas TI, servicios de recolección de data, operaciones de centros de llamadas;
e) gerencia y consultores comerciales, y auditores;
f) diseñadores y proveedores; por ejemplo, productos de software y sistemas TI;
g) limpieza, abastecimiento de alimentos (catering) y otros servicios de soporte abastecido externamente;

h) personal temporal, colocación de estudiantes y otros nombramientos casuales de corto plazo.

Estos acuerdos pueden ayudar a reducir los riesgos asociados con los grupos externos.

6.2.2 Tratamiento de la seguridad cuando se lidia con clientes

Control

Se debieran tratar todos los requerimientos de seguridad identificados antes de proporcionar a los clientes acceso a la información o activos de la organización.

Lineamiento de implementación

Se debieran considerar los siguientes términos de seguridad antes de proporcionar a los clientes acceso a cualquier activo de la organización (dependiendo del tipo y extensión de acceso dado, tal vez no se apliquen todos ellos):

a) protección de activos, incluyendo:
   1) procedimientos para proteger los activos de la organización, incluyendo información y software, y el manejo de las vulnerabilidades conocidas;
   2) procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data;
   3) integridad;
   4) restricciones sobre el copiado y divulgación de información;
b) descripción del producto o servicio a ser provisto;
c) las diferentes razones, requerimientos y beneficios para el acceso del cliente;
d) política de control de acceso, abarcando
   1) métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas;
   2) un proceso de autorización para el acceso y privilegios del usuario;
   3) un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado;
   4) un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;
e) acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad;
f) una descripción de cada servicio que debiera estar disponible;
g) el nivel objetivo del servicio y los niveles inaceptables del servicio;

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

i) las respectivas obligaciones de la organización y el cliente;

j) responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de data, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países (ver también 15.1);

k) derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor (ver 15.1.2) y protección de cualquier trabajo cooperativo (ver también 6.1.5).

Otra información

Los requerimientos de seguridad relacionados con el acceso del cliente a los activos organizacionales pueden variar considerablemente dependiendo de los medios de procesamiento de la información y la información a la cual se tiene acceso. Estos requerimientos de seguridad pueden ser tratados utilizando acuerdos con el cliente, los cuales contienen todos los riesgos identificados y los requerimientos de seguridad (ver 6.2.1).

Los acuerdos con los grupos externos también pueden involucrar a otras partes interesadas. Los acuerdos que otorgan acceso a grupos externos debieran incluir el permiso para la designación de otras partes elegibles y condiciones para su acceso y participación.

6.2.3 Tratamiento de la seguridad en acuerdos con terceros

Control

Los acuerdos o contratos con terceros que involucran el acceso, procesamiento, comunicación o manejo de la información o medios de procesamiento de información de la compañía, o agregan producto o servicios a los medios de procesamiento de información debieran abarcar todos los requerimientos de seguridad relevantes.

Lineamiento de implementación

El acuerdo debiera asegurar que no existan malos entendidos entre la organización y la otra parte. Las organizaciones debieran estar satisfechas con relación a la indemnización de las otras partes.

Se debieran considerar los siguientes términos a incluirse en el acuerdo para cumplir con los requerimientos de seguridad identificados (ver 6.2.1):

a) la política de seguridad de la información;

b) controles para asegurar la protección de los activos, incluyendo:

1) procedimientos para proteger los activos organizacionales, incluyendo información, software y hardware;
2) cualquier control y mecanismo de protección física requerido;
3) controles para asegurar la protección contra software malicioso (ver 10.4.1);
4) procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data;
4) controles para asegurar el retorno o destrucción de información y los activos al final de, o en un punto de tiempo acordado durante el acuerdo;
5) confidencialidad, integridad, disponibilidad y cualquier otra propiedad relevante (ver 2.1.5) de los activos;
6) restricciones sobre el copiado y divulgación de información, y la utilización de acuerdos de confidencialidad;

c) capacitación del usuario y administrador en métodos, procedimientos y seguridad;
d) asegurar la conciencia del usuario para las responsabilidades y problemas de la seguridad de la información;
e) provisión para la transferencia de personal, cuando sea apropiado;
f) responsabilidades relacionadas con la instalación y mantenimiento de hardware y software;
g) una estructura de reporte clara y formatos de reporte acordados;
h) un proceso claro y especificado de gestión de cambio;
i) política de control de acceso, abarcando:
   1) las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros;
   2) métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas;
   3) un proceso de autorización para el acceso y privilegios del usuario;
   4) un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso;
   5) un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado;
   6) un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;
j) acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad;

k) una descripción de cada servicio que debiera estar disponible, y una descripción de la información que debiera estar disponible junto con su clasificación de seguridad (ver 7.2.1);

l) el nivel objetivo del servicio y los niveles inaceptables del servicio;

m) una definición del criterio del desempeño verificable, su monitoreo y reporte;

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

o) el derecho de auditar las responsabilidades definidas en el acuerdo, el derecho que un tercero lleve a cabo la auditoria, y enumerar los derechos estatutarios de los auditores;

p) el establecimiento de un proceso escalonado para la solución de problemas;

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

r) las obligaciones respectivas de la organización y el cliente;

s) responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de data, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países (ver también 15.1);

t) derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor (ver 15.1.2) y protección de cualquier trabajo cooperativo (ver también 6.1.5).

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

v) condiciones para la negociación/terminación de los acuerdos:

   1) se debiera establecer un plan de contingencia en caso que alguna de las partes desee terminar la relación antes del fin del acuerdo;

   2) renegociación de acuerdos si los requerimientos de seguridad de la organización cambian;

   3) documentación actual de las listas de activos, licencias, acuerdos y derechos relacionados a ellos.

Otra información

Los acuerdos pueden variar considerablemente para las diferentes organizaciones y entre los diferentes tipos de terceras personas. Por lo tanto, se debiera tener cuidado de incluir todos los riesgos identificados y los requerimientos de seguridad (ver también 6.2.1) en los acuerdos. Cuando sea necesario, los controles y procedimientos requeridos se pueden expandir en un plan de gestión de seguridad.

Si la gestión de seguridad de la información es abastecida externamente, los acuerdos debieran tratar cómo estas terceras personas garantizarán mantener la seguridad adecuada,

tal como la define la evaluación del riesgo, y cómo se adaptará la seguridad para identificar y lidiar con los cambios en los riesgos.

Algunas de las diferencias entre el abastecimiento externo y otras formas de provisión de servicios de terceros incluyen la responsabilidad, planeación del período de transición e interrupción potencial de la operación durante este período, acuerdos para la planeación de contingencias, las revisiones debidas, y la recolección y manejo de información sobre incidentes de seguridad. Por lo tanto, es importante que la organización planee y maneje la transición a un acuerdo de abastecimiento externo y cuente con los procesos adecuados para manejar los cambios y los acuerdos de negociación/terminación.

En el acuerdo o contrato se necesitan considerar procedimientos para continuar el procesamiento en el evento que la tercera persona no pueda suministrar los servicios para evitar cualquier demora en acordar el reemplazo de los servicios.

Los acuerdos con terceros también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a terceros debieran incluir el permiso para designar a otras partes elegibles y las condiciones para su acceso y participación.

Generalmente, los acuerdos son principalmente desarrollados por la organización. En algunas circunstancias, puede haber ocasiones donde el acuerdo puede ser desarrollado e impuesto a la organización por una tercera persona. La organización necesita asegurarse que su propia seguridad no se vea necesariamente afectada por los requerimientos de terceros estipulados en los acuerdos impuestos.

7 Gestión de activos

7.1 Responsabilidad por los activos

Objetivo: Lograr y mantener una apropiada protección de los activos organizacionales. Todos los activos debieran ser inventariados y contar con un propietario nombrado. Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

7.1.1 Inventario de los activos

Control

Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes.

Lineamiento de implementación

Una organización debiera identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado.

Además, se debiera acordar y documentar la propiedad (ver 7.1.2) y la clasificación de la propiedad (ver 7.2) para cada uno de los activos. Basados en la importancia del activo, su valor comercial y su clasificación de seguridad, se debieran identificar los niveles de protección que se conmensuran con la importancia de los activos (se puede encontrar más información sobre cómo valorar los activos para representar su importancia en ISO/IEC TR 13335-3).

Otra información

Existen muchos tipos de activos, incluyendo:

a) información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
b) activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;
c) activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo;
d) servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;
e) personas, y sus calificaciones, capacidades y experiencia;
f) intangibles, tales como la reputación y la imagen de la organización.

Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los activos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos). El proceso de compilar un inventario de activos es un pre-requisito importante de la gestión del riesgo (ver también la Sección 4).

7.1.2 Propiedad de los activos

Control

Toda la información y los activos asociados con los medios de procesamiento de información debieran ser propiedad[2] de una parte designada de la organización.

Lineamiento de implementación

El propietario del activo debiera ser responsable de:

a) asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente;
b) definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignada a:

a) un proceso comercial;
b) un conjunto de actividades definido;
c) una aplicación; o
d) un conjunto de data definido.

Otra información

Se pueden delegar las tareas rutinarias; por ejemplo, a un custodio que supervisa el activo diariamente, pero la responsabilidad permanece con el propietario.

En los sistemas de información complejos podría ser útil designar grupos de activos, los cuales actúan juntos para proporcionar una función particular como "servicios". En este caso el propietario es responsable de la entrega del servicio, incluyendo el funcionamiento de los activos que los proveen.

[2] El término "propietario" identifica una persona o entidad que cuenta con la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término "propietario" no significa que la persona en realidad tenga algún derecho de propiedad sobre el activo.

7.1.3 Uso aceptable de los activos

Control

Se debieran identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

Lineamiento de implementación

Todos los empleados, contratistas y terceros debieran seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, incluyendo:

a) reglas para la utilización del correo electrónico e Internet (ver 10.8);
b) lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización (ver 11.7.1).

La gerencia relevante debiera proporcionar reglas o lineamientos específicos. Los empleados, contratistas y terceros que usan o tienen acceso a los activos de la organización debieran estar al tanto de los límites existentes para su uso de la información y los activos asociados con los medios y recursos del procesamiento de la información de la organización. Ellos debieran ser responsables por el uso que le den a cualquier recurso de procesamiento de información, y de cualquier uso realizado bajo su responsabilidad.

7.2 Clasificación de la información

Objetivo: Asegurar que la información reciba un nivel de protección apropiado. La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información. La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debiera utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

7.2.1 Lineamientos de clasificación

Control

Se debiera clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.

Lineamiento de implementación

Las clasificaciones y los controles de protección asociados para la información debieran tomar en cuenta las necesidades comerciales de intercambiar o restringir información y los impactos comerciales asociados con dichas necesidades.

Los lineamientos de clasificación debieran incluir protocolos para la clasificación inicial y la re-clasificación a lo largo del tiempo; en concordancia con alguna política pre-determinada de control de acceso (ver 11.1.1).

Debiera ser responsabilidad del propietario del activo (ver 7.1.2) definir la clasificación de un activo, revisarla periódicamente y asegurarse que se mantenga actualizada y en el nivel apropiado. La clasificación debiera tomar en cuenta el efecto de agregación mencionado en 10.7.2.

Se debiera tener en consideración el número de categorías de clasificación y los beneficios a obtenerse con su uso. Los esquemas demasiado complejos pueden volverse engorrosos y anti-económicos de utilizar o pueden volverse poco prácticos. Se debiera tener cuidado al interpretar los encabezados de la clasificación en los documentos de otras organizaciones, los cuales pueden tener definiciones diferentes para encabezados con el mismo nombre o nombre similares.

Otra información

Se puede evaluar el nivel de protección analizando la confidencialidad, integridad y disponibilidad, y cualquier otro requerimiento para la información considerada.

Con frecuencia, la información deja de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Se debieran tomar en cuenta estos aspectos, ya que la sobre-clasificación puede llevar a la implementación de controles innecesarios resultando en un gasto adicional.

Agrupar documentos con requerimientos de seguridad similares cuando se asignan niveles de clasificación podría ayudar a simplificar la tarea de clasificación.

En general, la clasificación dada a la información es una manera rápida para determinar cómo se está manejando y protegiendo la información.

7.2.2 Etiquetado y manejo de la información

Control

Se debiera desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

Lineamiento de implementación

Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos.

El output de los sistemas conteniendo información que es clasificada como sensible o crítica debiera llevar la etiqueta de clasificación apropiada (en el output). El etiquetado debiera reflejar la clasificación de acuerdo a las reglas establecidas en 7.2.1. Los ítems a considerarse incluyen reportes impresos, presentaciones en pantalla, medios de grabación (por ejemplo; cintas, discos, CDs), mensajes electrónicos y transferencia de archivos.

Para cada nivel de clasificación, se debiera definir los procedimientos de manejo seguros; incluyendo el procesamiento, almacenaje, transmisión, de-clasificación y destrucción. Esto también debiera incluir los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.

Los acuerdos con otras organizaciones que incluyen intercambio de información debieran incluir procedimientos para identificar la clasificación de esa información e interpretar las etiquetas de clasificación de otras organizaciones.

Otra información

El etiquetado y el manejo seguro de la información clasificada es un requerimiento clave para los acuerdos de intercambio de información. Las etiquetas físicas son una forma común de etiquetado. Sin embargo, algunos archivos de información, como documentos en forma electrónica, no pueden ser etiquetados físicamente y se necesitan medios electrónicos para el etiquetado. Por ejemplo, la etiqueta de notificación puede aparecer en la pantalla. Cuando no es factible el etiquetado, se pueden aplicar otros medios para designar la clasificación de la información; por ejemplo, mediante procedimientos o meta-data.

8 Seguridad de recursos humanos

8.1 Antes del empleo[3]

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios. Las responsabilidades de seguridad debieran ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo. Los antecedentes de todos los candidatos al empleo, contratistas y terceros debieran ser adecuadamente investigados, especialmente para los trabajos confidenciales. Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información debieran firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.

8.1.1 Roles y responsabilidades

Control

Se debieran definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

Lineamiento de implementación

Los roles y responsabilidades debieran incluir requerimientos para:

a) implementar y actuar en concordancia con las políticas de seguridad de la información de la organización (ver 5.1);
b) proteger los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada;
c) ejecutar procesos o actividades de seguridad particulares;
d) asegurar que se asigne a la persona la responsabilidad por las acciones tomadas;

[3] Explicación: Aquí la palabra "empleo" se utiliza para abarcar las siguientes situaciones diversas:
Empleo de personas (temporal o permanente), asignación de roles de trabajo, asignación de contratos y la terminación de cualquiera de estos acuerdos.

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

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

Otra información

Se pueden utilizar las descripciones del puesto para documentar los roles y responsabilidades de seguridad. También se debieran definir y comunicar claramente los roles y responsabilidades para las personas no contratadas a través del proceso de empleo de la organización; por ejemplo, a través de una tercera organización.

8.1.2 Investigación de antecedentes

Control

Los chequeos de verificación de antecedentes de todos los candidatos para empleo, contratistas y terceros debieran llevarse a cabo en concordancia con las leyes, regulaciones y ética relevantes; y debieran ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Lineamiento de implementación

Los chequeos de verificación debieran tomar en cuenta la legislación relevante con relación a la privacidad de la data personal y/o empleo; y cuando sea permitido, debiera incluir lo siguiente:

a) disponibilidad de referencias de carácter satisfactorias; por ejemplo, una comercial y una personal;
b) un chequeo del curriculum vitae del postulante (buscando integridad y exactitud);
c) confirmación de las calificaciones académicas y profesionales mencionadas;
d) chequeo de identidad independiente (pasaporte o documento similar);
e) chequeos más detallados, como chequeos de crédito o chequeos de récords criminales.

Cuando un puesto de trabajo, sea un nombramiento inicial o un ascenso, involucra que la persona tenga acceso a los medios de procesamiento de información, y en particular si las personas manejan información confidencial; por ejemplo, información financiera o información altamente confidencial; la organización también debiera considerar chequeos más detallados.

Los procedimientos debieran definir los criterios y limitaciones para los chequeos de verificación; por ejemplo, quién es elegible para realizar la investigación de antecedentes, cómo, cuándo y porqué se llevan a cabo los chequeos de verificación.

Se debiera llevar a cabo un proceso de investigación de antecedentes para los contratistas y terceras personas. Cuando los contratistas son provistos a través de una agencia, el contrato con la agencia debiera especificar claramente las responsabilidades de la agencia con relación a la investigación de antecedentes y los procedimientos de notificación que se necesitan seguir si no se ha completado la investigación de antecedentes o si los resultados dan causa de duda o inquietud.

La información de todos los candidatos considerados para puestos dentro de la organización debiera ser recolectada y manejada en concordancia con cualquier legislación apropiada existente en la jurisdicción relevante. Dependiendo de la legislación aplicable, los candidatos debieran ser previamente informados sobre las actividades de investigación de antecedentes.

8.1.3 Términos y condiciones del empleo

Control

Como parte de su obligación contractual; los usuarios empleados, contratistas y terceros debieran aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual debiera establecer sus responsabilidades y las de la organización para la seguridad de la información.

Lineamiento de implementación

Los términos y condiciones de empleo debieran reflejar la política de seguridad de la organización, además de aclarar y establecer:

a) que todos los usuarios empleados, contratistas y terceros que tienen acceso a información sensible debieran firmar un acuerdo de confidencialidad o no-divulgación antes de otorgarles acceso a los medios de procesamiento de la información;
b) las responsabilidades y derechos de los empleados, contratistas y cualquier otro usuario; por ejemplo, con relación a las leyes de derecho de autoría y legislación de protección de data (ver también 15.1.1 y 15.1.2);
c) las responsabilidades para la clasificación de la información y la gestión de los activos organizacionales asociadas con los sistemas y servicios de información manejados por el empleado, contratista o tercera persona (ver también 7.2.1 y 10.7.3);

d) responsabilidades del usuario empleado, contratista o tercera persona con relación al manejo de la información recibida de otras compañías o partes externas;

e) las responsabilidades de la organización por el manejo de la información personal, incluyendo la información personal creada como resultado de, o en el curso de, el empleo con la organización (ver también 15.1.4);

f) las responsabilidades que se extienden fuera del local de la organización y fuera del horario normal de trabajo; por ejemplo, en el caso del trabajo en casa (ver también 9.2.5 y 11.7.1);

g) las acciones a tomarse si el usuario empleado, contratista o tercera persona no cumple los requerimientos de seguridad de la organización (ver también 8.2.3).

La organización debiera asegurarse que los usuarios empleados, contratistas y terceras personas acepten los términos y condiciones concernientes a la seguridad de la información apropiada según la naturaleza y extensión del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información.

Cuando fuese apropiado, las responsabilidades contenidas dentro de los términos y condiciones del empleo debieran continuar por un período definido después de terminado el empleo (ver también 8.3).

Otra información

Se puede utilizar un código de conducta para abarcar las responsabilidades del usuario empleado, contratista y tercera persona con relación a la confidencialidad, protección de data, ética, uso apropiado del equipo y medios de la organización; así como las prácticas respetables esperadas por la organización. Los usuarios contratistas o terceras personas pueden estar asociados con una organización externa que a su vez puede requerir que firmen un contrato en representación de la persona contratada.

8.2 Durante el empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano. Se debieran definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro de la organización.

Se debiera proporcionar a todos los usuarios empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad. Se debiera establecer un proceso disciplinario normal para manejar las fallas en la seguridad.

8.2.1 Responsabilidades de la gerencia

Control

La gerencia debiera requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.

Lineamiento de implementación

Las responsabilidades de la gerencia debieran incluir asegurar que los usuarios empleados, contratistas y terceras personas:

a) estén apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información;
b) reciban lineamientos para establecer las expectativas de seguridad de su rol dentro de la organización;
c) estén motivados para cumplir con las políticas de seguridad de la organización;
d) lograr un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro de la organización (ver también 8.2.2);
e) cumplan con los términos y condiciones de empleo, los cuales incluyen la política de seguridad de la información de la organización y los métodos de trabajo apropiados;
f) continúen teniendo las capacidades y calificaciones apropiadas.

Otra información

Si los usuarios empleados, contratistas y terceras personas no son conscientes de sus responsabilidades de seguridad, ellos pueden causar un daño considerable a la organización. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

Una gerencia deficiente puede causar que el personal se sienta subestimado resultando en un impacto de seguridad negativo para la organización. Por ejemplo, una gerencia deficiente

puede llevar a que la seguridad sea descuidada o a un potencial uso inadecuado de los activos de la organización.

8.2.2 Conocimiento, educación y capacitación en seguridad de la información

Control

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

Lineamiento de implementación

La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.

La capacitación constante debiera incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales, así como la capacitación en el uso correcto de los medios de procesamiento de información; por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios (ver 8.2.3).

Otra información

Las actividades de conocimiento, educación y capacitación debieran ser adecuados y relevantes para el rol, responsabilidades y capacidades de la persona, y debieran incluir información sobre amenazas conocidas, a quién contactar para mayor consultoría sobre seguridad y los canales apropiados para reportar los incidentes de seguridad de información (ver también 13.1).

La capacitación para aumentar la conciencia y conocimiento tiene como objetivo permitir a las personas reconocer los problemas e incidentes de la seguridad de la información, y responder de acuerdo a las necesidades de su rol en el trabajo.

8.2.3 Proceso disciplinario

Control

Debiera existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.

Lineamiento de implementación

El proceso disciplinario no debiera iniciarse sin una verificación previa de la ocurrencia del incumplimiento de la seguridad (ver también 13.2.3 para la recolección de evidencia).

El proceso disciplinario formal debiera asegurar el tratamiento correcto y justo para los empleados sospechosos de cometer incumplimientos de la seguridad. El proceso disciplinario debiera proporcionar una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio, si esta es la primera ofensa, si el culpable fue apropiadamente capacitado, la legislación relevante, contratos comerciales y otros factores que se puedan requerir. En los casos serios de dolo, el proceso debiera permitir la remoción inmediata de los debierares, derechos de acceso y privilegios, y si fueses necesario, acompañar inmediatamente a la personas fuera del local.

Otra información

El proceso disciplinario también se puede utilizar como un disuasivo para evitar que los usuarios empleados, contratistas y terceras personas violen las políticas y procedimientos de seguridad organizacionales, y cualquier otro incumplimiento de la seguridad.

8.3 Terminación o cambio de empleo

Objetivo: Asegurar que los usuarios empleados, contratistas y terceras personas salgan de la organización o cambien de empleo de una manera ordenada. Se debieran establecer las responsabilidades para asegurar que la salida de la organización del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso. Los cambios en las responsabilidades y empleos dentro de la organización se pueden manejar como la terminación de la responsabilidad o empleo respectivo en concordancia con esta sección, y cualquier empleo nuevo debiera ser manejado tal como se describe en la sección 8.1.

8.3.1 Responsabilidades de terminación

Control

Se debieran definir y asignar claramente las responsabilidades de realizar la terminación del empleo o el cambio de empleo.

Lineamiento de implementación

La comunicación de las responsabilidades de terminación debieran incluir requerimientos de seguridad constantes y responsabilidades legales y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad (ver 6.1.5) y los términos y condiciones de empleo (ver 8.1.3) continuando durante un período después de terminado el empleo del usuario empleado, contratista o tercera persona.

Las responsabilidades y debierares aún válidos después de la terminación del empleo debieran estar contenidos en los contratos del empleado, contratista o tercera persona.

Los cambios en la responsabilidad o empleo debieran ser manejados como la terminación de la responsabilidad o empleo respectivo, y la responsabilidad o empleo nuevo debiera ser controlado tal como se describe en la cláusula 8.1.

Otra información

La función de Recursos Humanos generalmente es responsable del proceso de terminación en general y trabaja junto con el gerente supervisor de la persona que se va para manejar los aspectos de seguridad de los procedimientos relevantes. En el caso del contratista, este proceso de responsabilidad de terminación puede ser realizado por la agencia responsable por el contratista, y en el caso de otro usuario podría ser manejado por su organización.

Puede ser necesario informar a los usuarios empleados, contratistas o terceras personas de los cambios en el personal y los acuerdos de operación.

8.3.2 Devolución de los activos

Control

Todos los usuarios empleados, contratistas y terceras personas debieran devolver todos los activos de la organización que tengan en su posesión a la terminación de su empleo, contrato o acuerdo.

Lineamiento de implementación

El proceso de terminación debiera ser formalizado para incluir la devolución de todo el software, documentos corporativos y equipo entregado previamente. También se debieran devolver otros activos organizacionales como dispositivos de cómputo móviles, tarjetas de

crédito, tarjetas de acceso, software, manuales e información almacenada en medios electrónicos.

En los casos donde el usuario empleado, contratista o tercera persona compra el equipo de la organización o utiliza su propio equipo, se debieran seguir procedimientos para asegurar que toda la información relevante sea transferida a la organización y sea adecuadamente borrada del equipo (ver también 10.7.1).

En los casos donde el usuario empleado, contratista o tercera persona tiene conocimiento que es importante para las operaciones actuales, esa información debiera ser documentada y transferida a la organización.

8.3.3 Retiro de los derechos de acceso

Control

Los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información debieran ser retirados a la terminación de su empleo, contrato o acuerdo, o debieran ser reajustados de acuerdo al cambio.

Lineamiento de implementación

A la terminación, se debieran reconsiderar los derechos de acceso de una persona a los activos asociados con los sistemas y servicios de información. Esto determinará si es necesario retirar los derechos de acceso. Los cambios de un empleo se debieran reflejar en el retiro de todos los derechos de acceso que no fueron aprobados para el empleo nuevo. Los derechos de acceso que se debieran retirar o adaptar incluyen el acceso físico y lógico, llaves, tarjetas de identificación, medios de procesamiento de información (ver también 11.2.4), suscripciones; y el retiro de cualquier documentación que identifique a la persona como miembro actual de la organización. Si un usuario empleado, contratista o tercera persona que está dejando la organización conoce las claves secretas para las cuentas aún activas, estas debieran ser cambiadas a la terminación o cambio del empleo, contrato o acuerdo.

Los derechos de acceso para los activos de información y los medios de procesamiento de información se debieran reducir o retirar antes de la terminación o cambio del empleo, dependiendo de la evaluación de los factores de riesgo como:

a) si la terminación o cambio es iniciado por el usuario empleado, contratista o tercera persona, o por la gerencia y la razón de la terminación;
b) las responsabilidades actuales del usuario empleado, contratista o cualquier otro usuario;

c) el valor de los activos actualmente disponibles.

Otra información

En ciertas circunstancias, los derechos de acceso pueden ser asignados sobre la base de estar disponibles para más personas que el usuario empleado, contratista o tercera persona; por ejemplo, los IDs del grupo. En tales circunstancias, las personas que se van debieran ser retiradas de las listas de acceso del grupo y se debieran realizar arreglos para comunicar a todos los otros usuarios empleados, contratistas y terceros involucrados para que ya no compartan esta información con la persona que se va.

En casos de terminaciones iniciadas por la gerencia, los empleados, contratistas o terceros descontentos pueden corromper la información deliberadamente o sabotear los medios de procesamiento de la información. En caso de las personas que renuncian, pueden tratar de recolectar información para su uso futuro.

9 Seguridad física y ambiental

9.1 Áreas seguras

Objetivo: Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización. Los medios de procesamiento de información crítica o confidencial debieran ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Debieran estar físicamente protegidos del acceso no autorizado, daño e interferencia.

9.1.1 Perímetro de seguridad física

Control

Se debieran utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

Lineamiento de implementación

Cuando sea apropiado, se debieran considerar e implementar los siguientes lineamientos para los perímetros de seguridad físicos:

a) los perímetros de seguridad debieran estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo;

b) los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser físicamente sólidos (es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado); las paredes externas del local debieran ser una construcción sólida y todas las puertas externas debieran estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes, etc.; las puertas y ventanas debieran quedar aseguradas cuando están desatendidas y se debiera considerar una protección externa para las ventas, particularmente en el primer piso;

c) se debiera contar con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado;

d) cuando sea aplicable, se debieran elaborar las barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental;

e) todas las puertas de emergencia en un perímetro de seguridad debieran contar con alarma, debieran ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales; debieran operar en concordancia con el código contra-incendios local de una manera totalmente segura;

f) se debieran instalar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas debieran contar con alarma en todo momento; también se debiera proveer protección para otras áreas; por ejemplo, el cuarto de cómputo o cuarto de comunicaciones;

g) los medios de procesamiento de información manejados por la organización debieran estar físicamente separados de aquellas manejadas por terceros.

Otra información

La protección física se puede lograr creando una o más barreras físicas alrededor de los locales de la organización y los medios de procesamiento de información. El uso de las

múltiples barreras proporciona protección adicional, para que la falla de una barrera no signifique que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina con llave, o varias habitaciones rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad dentro del perímetro de seguridad.

Se debiera prestar consideración especial a la seguridad de acceso físico que se debiera dar a los edificios donde se alojan múltiples organizaciones.

9.1.2 Controles de ingreso físico

Control

Las áreas seguras debieran protegerse mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos:

a) se debiera registrar la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes debieran ser supervisados a no ser que su acceso haya sido previamente aprobado; sólo se les debiera permitir acceso por propósitos específicos y autorizados y se debieran emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia;
b) el acceso a áreas donde se procesa o almacena información sensible se debiera controlar y restringir sólo a personas autorizadas; se debieran utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos;
c) se debiera requerir que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible y se debiera notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado y cualquiera que no use una identificación visibles;
d) al personal de servicio de apoyo de terceros se le debiera otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado y monitoreado;
e) los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario (ver 8.3.3).

9.1.3 Asegurar las oficinas, habitaciones y medios

Control

Se debiera diseñar y aplicar la seguridad física para las oficinas, habitaciones y medios.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para asegurar las oficinas, habitaciones y medios:

a) se debiera tener en cuenta los estándares y regulaciones de sanidad y seguridad relevantes;
b) se debieran localizar los medios claves para evitar el acceso del público;
c) donde sea aplicables, los edificios debieran ser discretos y dar una indicación mínima de su propósito, sin carteles obvios dentro y fuera del edificio que indiquen la presencia de actividades de procesamiento de información;
d) los directorios y teléfonos internos que identifiquen la ubicación de los medios de procesamiento de la información no debieran estar accesibles al público.

9.1.4 Protección contra amenazas externas e internas

Control

Se debiera asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Lineamiento de implementación

Se debiera prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debieran considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles debieran ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no debiera almacenarse en el área asegurada;
b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;
c) se debiera proporcionar equipo contra-incendios ubicado adecuadamente.

9.1.5 Trabajo en áreas aseguradas

Control

Se debiera diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos:

a) el personal debiera estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer;
b) se debiera evitar el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos;
c) las áreas aseguradas vacías debieran ser cerradas físicamente bajo llave y revisadas periódicamente;
d) no se debiera permitir equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea autorizado.

Los arreglos para trabajar en las áreas aseguradas incluyen controles para los empleados, contratistas y terceros que trabajen en el área asegurada, así como otras actividades de terceros que allí se realicen.

9.1.6 Áreas de acceso público, entrega y carga

Control

Se debieran controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, si fuese posible, debieran aislarse de los medios de procesamiento de información para evitar el acceso no autorizado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos:

a) el acceso al área de entrega y carga desde fuera del edificio se debiera restringir al personal identificado y autorizado;
b) se debiera diseñar el área de entrega y carga de manera que se pueda descargar los suministros sin que el personal de entrega tenga acceso a otras partes del edificio;

c) las puertas externas del área de entrega y carga debieran estar aseguradas cuando se abren las puertas internas;
d) se debiera inspeccionar el material que ingresa para evitar amenazas potenciales (ver 9.2.1d) antes que el material sea trasladado del área de entrega y carga al punto de uso;
e) se debiera registrar el material que ingresa en concordancia con los procedimientos de gestión de activos (ver también 7.1.1) a su ingreso al local;
f) cuando fuese posible, los embarques que ingresan y salen debieran estar segregados.

9.2 Equipo de seguridad

Objetivo: Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

Se debiera proteger el equipo de amenazas físicas y ambientales.

La protección del equipo (incluyendo aquel utilizado fuera del local y la eliminación de propiedad) es necesaria para reducir el riesgo de acceso no-autorizado a la información y proteger contra pérdida o daño. Esto también debiera considerar la ubicación y eliminación del equipo. Se pueden requerir controles especiales para proteger el equipo contra amenazas físicas, y salvaguardar los medios de soporte como el suministro eléctrico y la infraestructura del cableado.

9.2.1 Ubicación y protección del equipo

Control

Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no-autorizado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para la protección del equipo:

a) el equipo se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;
b) los medios de procesamiento de la información que manejan data confidencia debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el

riesgo que la información sea vista por personas no autorizadas durante su uso; y se debieran asegurar los medios de almacenaje para evitar el acceso no autorizado;

c) se debieran aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;

d) se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

e) se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;

f) se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información;

g) se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;

h) se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;

i) se debiera proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

9.2.2 Servicios públicos de soporte

Control

Se debiera proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Lineamiento de implementación

Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; debieran ser adecuados para los sistemas que soportan. Los servicios públicos de soporte debieran ser inspeccionados regularmente y, conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla. Se debiera proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.

Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas. Los planes de contingencia para la energía debieran abarcar la acción a tomarse en el caso de una

falla de energía prolongada. Se debiera considerar un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada. Se debiera tener disponible un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado. El equipo UPS y los generados se debieran chequear regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante. Además, se debiera considerar al uso de múltiples fuentes de energía, si el local es grande, una subestación de energía separada.

Se debieran colocar interruptores de energía de emergencia cerca de las salidas de emergencia en las habitaciones donde se encuentra el equipo para facilitar el cierre del paso de corriente en caso de una emergencia. Se debiera proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.

El suministro de energía debiera ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y los sistemas contra-incendios (donde se utilicen). El mal funcionamiento del sistema de suministro de agua pude dañar el equipo y evitar que el sistema contra-incendios funcione adecuadamente. Se debiera evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.

El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz. Los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

Otra información

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

9.2.3 Seguridad del cableado

Control

El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para la seguridad del cableado:

a) cuando sea posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información debieran ser subterráneas o debieran estar sujetas a una alternativa de protección adecuada;

b) el cableado de la red debiera estar protegido contra intercepciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas;

c) los cables de energía debieran estar separados de los cables de comunicaciones para evitar la interferencia;

d) se debieran utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados;

e) se debiera utilizar una lista de empalmes documentados para reducir la posibilidad de error;

f) para sistemas sensibles o críticos se debieran considerar más controles como:

1) la instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación;

2) el uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada;

3) el uso de cableado de fibra óptica;

4) el uso de un escudo electromagnético para proteger los cables;

5) la iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves;

6) acceso controlado para empalmar los paneles y los cuartos de cableado.

9.2.4 Mantenimiento de equipo

Control

Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para el mantenimiento de equipo:

a) el equipo se debiera mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor;

b) sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo;

c) se debieran mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo;

d) se debieran implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario, se debiera

revisar la información confidencial del equipo, o se debiera verificar al personal de mantenimiento;

e) se debieran cumplir con todos los requerimientos impuestos por las pólizas de seguros.

9.2.5 Seguridad del equipo fuera del local

Control

Se debiera aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

Lineamiento de implementación

Sin importar la propiedad, el uso de cualquier equipo de procesamiento de la información fuera del local de la organización debiera ser autorizado por la gerencia.

Se debieran considerar los siguientes lineamientos para la protección del equipo fuera del local:

a) el equipo y medios sacados del local nunca debiera ser dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles debieran ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada;

b) se debieran observar en todo momento las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos;

c) se debieran determinar controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío, controles de acceso para las computadoras y una comunicación segura con la oficina (ver también ISO/IEC 18028 Seguridad de Redes);

d) se debiera contar con un seguro adecuado para proteger el equipo fuera del local.

Los riesgos de seguridad; por ejemplo, daño, robo o intercepción; puede variar considerablemente entre los locales y se debiera tomar esto en cuenta para determinar los controles más apropiados.

Otra información

El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes u otras

formas que se utilicen para trabajar desde casa o se transporte fuera de local normal de trabajo.

9.2.6 Seguridad de la eliminación o re-uso del equipo

Control

Se debieran chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

Lineamiento de implementación

Los dispositivos que contienen información confidencial debieran ser físicamente destruidos o se debieran destruir, borrar o sobre-escribir la información utilizando técnicas que hagan imposible recuperar la información original, en lugar de simplemente utilizar la función estándar de borrar o formatear.

Otra información

Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

La información puede verse comprometida a través de una eliminación descuidada o el re-uso del equipo (ver también 10.7.2).

9.2.7 Retiro de propiedad

Control

El equipo, información o software no debiera retirarse sin autorización previa.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos:

a) no se debiera retirar equipo, información o software sin autorización previa;

b) los usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local debieran estar claramente identificados;

c) se debieran establecer límites de tiempo para el retiro del equipo y se debieran realizar un chequeo de la devolución;

d) cuando sea necesario y apropiado, el equipo debiera ser registrado como retirado del local y se debiera registrar su retorno.

Otra información

También se pueden realizar chequeos inesperados para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al local. Estos chequeos inesperados debieran ser llevados a cabo en concordancia con la legislación y regulaciones relevantes. Las personas debieran saber que se llevan a cabo chequeos inesperados, y los chequeos se debieran realizar con la debida autorización de los requerimientos legales y reguladores.

10 Gestión de las comunicaciones y operaciones

10.1 Procedimientos y responsabilidades operacionales

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información. Se debieran establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados. Cuando sea apropiado, se debiera implementar la segregación de debierares para reducir el riesgo de negligencia o mal uso deliberado del sistema.

10.1.1 Procedimientos de operación documentados

Control

Los procedimientos de operación se debieran documentar, mantener y poner a disposición de todos los usuarios que los necesiten.

Lineamiento de implementación

Se debieran preparar procedimientos documentados para las actividades del sistema asociadas con los medios de procesamiento de la información y comunicación; tales como procedimientos para encender y apagar computadoras, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de cómputo, manejo del correo y seguridad.

Los procedimientos de operación debieran especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

a) procesamiento y manejo de información;
b) copia de seguridad o respaldo (ver 10.5);
c) requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos;
d) instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema (ver 11.5.4);
e) contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas;
f) instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos (ver 10.10);
g) procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema;
h) la gestión de la información del rastro de auditoría y registro del sistema (ver 10.10).

Los procedimientos de operación y los procedimientos documentados para las actividades del sistema debieran ser tratados como documentos formales y cambios autorizados por la gerencia. Donde sea técnicamente factible, los sistemas de información debieran ser manejados consistentemente, utilizando los mismos procedimientos, herramientas y utilidades.

10.1.2 Gestión del cambio

Control

Se debieran controlar los cambios en los medios y sistemas de procesamiento de la información.

Lineamiento de implementación

Los sistemas operacionales y el software de aplicación debieran estar sujetos a un estricto control gerencial del cambio.

En particular, se debieran considerar los siguientes ítems:

a) identificación y registro de cambios significativos;
b) planeación y prueba de cambios;
c) evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad,

d) procedimiento de aprobación formal para los cambios propuestos;
e) comunicación de los detalles del cambio para todos las personas relevantes:
f) procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.

Se debieran establecer las responsabilidades y procedimientos gerenciales formales para asegurar un control satisfactorio de todos los cambios en el equipo, software o procedimientos. Cuando se realizan los cambios, se debiera mantener un registro de auditoría conteniendo toda la información relevante.

Otra información

El control inadecuado de los cambios en los medios de procesamiento de la información y los sistemas es una causa común de fallas en el sistema o en la seguridad. Los cambios en el ambiente operacional, especialmente cuando se transfiere un sistema de la etapa de desarrollo a la etapa operacional, pueden influir en la confiabilidad de la aplicación (ver también 12.5.1).

Los cambios en los sistemas de operación sólo se debieran realizar cuando existe una razón comercial válida para hacerlo, como un incremento en el riesgo para el sistema. Actualizar los sistemas con la versión más moderna del sistema de operación o aplicación no es siempre lo mejor para el negocio ya que podría introducir más vulnerabilidades e inestabilidad que la versión actual. También puede existir la necesidad de mayor capacitación, costos de licencias, soporte, mantenimiento y gastos generales; y también hardware nuevo especialmente durante la migración.

10.1.3 Segregación de los deberes

Control

Los debierares y áreas de responsabilidad debieran estar segregados para reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la organización.

Lineamiento de implementación

La segregación de los debierares es un método para reducir el riesgo de un mal uso accidental o deliberado del sistema. Se debiera tener cuidado que nadie pueda tener acceso, modificar o utilizar los activos sin autorización o detección. Se debiera separar la iniciación de un evento

de su autorización. Se debiera considerar la posibilidad de colusión en el diseño de los controles.

Las organizaciones pequeñas pueden encontrar difícil de lograr la segregación de debierares, pero se debiera aplicar el principio mientras sea posible y practicable. Cuando es difícil de segregar, se debieran considerar otros controles como el monitoreo de actividades, rastros de auditoría y supervisión gerencial. Es importante que la auditoría de seguridad se mantenga independiente.

10.1.4 Separación de los medios de desarrollo, prueba y operación

Control

Los medios de desarrollo, prueba y operación debieran estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional.

Lineamiento de implementación

Se debiera identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales y se debieran implementar los controles apropiados.

Se debieran considerar los siguientes ítems:

a) se debieran definir y documentar las reglas para la transferencia de software del estado de desarrollo al operacional;
b) los software de desarrollo y operacional debieran correr en sistemas o procesadores de cómputo, y en diferentes dominios o directorios;
c) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no debieran ser accesibles desde los sistemas operacionales cuando no se requieran;
d) el ambiente del sistema de prueba debiera emular el ambiente del sistema operacional lo más estrechamente posible;
e) los usuarios debieran utilizar perfiles de usuario diferentes para los sistemas operacionales y de prueba, y los menús debieran mostrar los mensajes de identificación apropiados para reducir el riesgo de error.
f) la data confidencial no debiera ser copiada en el ambiente del sistema de prueba (ver 12.4.2).

Otra información

Las actividades de desarrollo y prueba pueden ser problemas serios; por ejemplo, una modificación no deseada de los archivos o el ambiente del sistema, o una falla en el sistema. En este caso, existe la necesidad de mantener un ambiente conocido y estable en el cual realizar una prueba significativa y evitar un inadecuado acceso del encargado del desarrollo.

Cuando el personal de desarrollo y prueba tiene acceso al sistema operacional y su información, ellos pueden introducir un código no-autorizado o no-probado o alterar la data de operación. En algunos sistemas esta capacidad puede ser mal utilizada para cometer fraude, o introducir un código no-probado o malicioso, el cual puede causar serios problemas operacionales.

Los encargados del desarrollo y las pruebas también podrían ser una amenaza para la confidencialidad de la información operacional. Las actividades de desarrollo y prueba pueden causar daños no-intencionados al software o la información si es que comparten el mismo ambiente de cómputo. Por lo tanto, es deseable separar los medios de desarrollo, prueba y operación para reducir el riesgo de un cambio accidental o acceso no-autorizado al software operacional y la data del negocio (ver también 12.4.2 para la protección de la data de prueba).

10.2 Gestión de la entrega del servicio de terceros

Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros. La organización debiera chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

10.2.1 Entrega del servicio

Control

Se debiera asegurar que los controles de seguridad, definiciones del servicio y niveles de entrega incluidos en el acuerdo de entrega del servicio de terceros se implementen, operen y mantengan.

Lineamiento de implementación

La entrega del servicio por un tercero debiera incluir los acuerdos de seguridad pactados, definiciones del servicio y aspectos de la gestión del servicio. En caso de los acuerdos de abastecimiento externo, la organización debiera planear las transiciones necesarias (de

información, medios de procesamiento de la información y cualquier otra cosa que necesite trasferirse), y debiera asegurar que se mantenga la seguridad a través del período de transición.

La organización debiera asegurar que la tercera persona mantenga una capacidad de servicio suficiente junto con los planes de trabajo diseñados para asegurar que se mantengan los nivel de continuidad del servicio después de fallas importantes en el servicio o un desastre (ver 14.1).

10.2.2 Monitoreo y revisión de los servicios de terceros

Control

Los servicios, reportes y registros provistos por terceros debieran ser monitoreados y revisados regularmente, y se debieran llevar a cabo auditorías regularmente.

Lineamiento de implementación

El monitoreo y revisión de los servicios de terceros debiera asegurar que se cumplan los términos y condiciones de seguridad de los acuerdos, y que se manejen apropiadamente los incidentes y problemas de seguridad de la información. Esto debiera involucrar una relación y proceso de gestión de servicio entre la organización y la tercera persona para:

a) monitorear los niveles de desempeño del servicio para chequear adherencia con los acuerdos;
b) revisar de los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme lo requieran los acuerdos;
c) proporcionar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la organización conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte;
d) revisar los rastros de auditoría de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado;
e) resolver y manejar cualquier problema identificado.

La responsabilidad de manejar la relación con terceros se debiera asignar a una persona o equipo de gestión de servicios. Además, la organización debiera asegurar que los terceros asignen responsabilidad para el chequeo del cumplimiento de los requerimientos de los acuerdos. Se debieran poner a disposición las capacidades y recursos técnicos para monitorear los requerimientos del acuerdo (ver 6.2.3), en particular si se cumplen los

requerimientos de seguridad de la información. Se debiera tomar la acción apropiada cuando se observan deficiencias en la entrega del servicio.

La organización debiera mantener el control y la visibilidad general suficiente en todos los aspectos de seguridad con relación a la información confidencial o crítica o los medios de procesamiento de la información que la tercera persona ingresa, procesa o maneja. La organización debiera asegurarse de mantener visibilidad en las actividades de seguridad como la gestión del cambio, identificación de vulnerabilidades y reporte/respuesta de un incidente de seguridad a través de un proceso, formato y estructura de reporte definidos.

Otra información

En caso de abastecimiento externo, la organización necesita estar al tanto que la responsabilidad final de la información procesada por un proveedor externo se mantenga en la organización.

10.2.3 Manejo de cambios en los servicios de terceros

Control

Se debieran manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad de la información existentes teniendo en cuenta el grado crítico de los sistemas y procesos del negocio involucrados y la re-evaluación de los riesgos.

Lineamiento de implementación

El proceso de manejar los cambios en el servicio de terceros necesita tomar en cuenta:

a) los cambios realizados por la organización para implementar:
   1) aumentos los servicios ofrecidos actualmente;
   2) desarrollo de cualquier aplicación y sistema nuevo;
   3) modificaciones o actualizaciones de las políticas y procedimientos de la organización;
   4) controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad;
      1) cambios en los servicios de terceros para implementar:
      1) cambios y mejoras en las redes;
      2) uso de tecnologías nuevas;
      3) adopción de productos nuevos o versiones más modernas;

4) desarrollo de herramientas y ambientes nuevos;
5) cambios en la ubicación física de los medios del servicio;
6) cambio de vendedores.

10.3 Planeación y aceptación del sistema

Objetivo: Minimizar el riesgo de fallas en el sistema. Se requiere de planeación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido. Se debieran realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema. Se debieran establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

10.3.1 Gestión de la capacidad

Control

Se debiera monitorear, afinar el uso de los recursos y se debieran realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

Lineamiento de implementación

Se debieran identificar los requerimientos de capacidad de cada actividad nueva y en proceso. Se debieran aplicar la afinación y monitoreo del sistema para asegurar y, cuando sea necesario, mejorar la disponibilidad y eficiencia de los sistemas. Se debieran establecer detectives de controles para indicar los problemas en el momento debido. Las proyecciones de requerimientos futuros debieran tomar en cuenta los requerimientos de los negocios y sistemas nuevos y las tendencias actuales y proyectadas en las capacidades de procesamiento de la información de la organización.

Se debiera prestar atención particular atención a cualquier recurso con tiempo de espera largos de abastecimiento o costos altos; por lo tanto, los gerentes debieran monitorear la utilización de los recursos claves del sistema. Ellos debieran identificar las tendencias de uso, particularmente en relación con las aplicaciones comerciales o las herramientas del sistema de información gerencial.

Los gerentes debieran utilizar esta información para identificar y evitar cuellos de botella potenciales y depender del personal clave que podría presentar una amenaza a la seguridad o los servicios del sistema, y debieran planear la acción apropiada.

10.3.2 Aceptación del sistema

Control

Se debiera establecer el criterio de aceptación de los sistemas de información nuevos, actualizaciones o versiones nuevas y se debieran realizar pruebas adecuadas del sistema(s) durante el desarrollo y antes de su aceptación.

Lineamiento de implementación

Los gerentes debieran asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos estén claramente definidos, aceptados, documentados y probados. Los sistemas de información nuevos, las actualizaciones y las versiones nuevas debieran migrar a la producción después de obtener la aceptación formal. Se debieran considerar los siguientes ítems antes de proporcionar la aceptación formal:

a) el desempeño y los requerimientos de capacidad de la computadora;
b) procedimientos para la recuperación tras errores y reinicio, y planes de contingencia;
c) preparación y prueba de los procedimientos de operación rutinarios para estándares definidos;
d) el conjunto de controles de seguridad acordados y aceptados;
e) procedimientos manuales efectivos;
f) arreglos para la continuidad del negocio (ver 14.1);
g) evidencia que la instalación del sistema nuevo no afectará adversamente los sistemas existentes, particularmente en las horas picos del procesamiento, como fin de mes;
h) evidencia que se está tomando en consideración el efecto que tiene el sistema nuevo en la seguridad general de la organización;
i) capacitación para la operación o uso de los sistemas nuevos;
j) facilidad de uso, ya que esto afecta el desempeño del usuario y evita el error humano.

Para los desarrollos nuevos importantes, la función de las operaciones y los usuarios debieran ser consultados en todas las etapas del proceso del desarrollo para asegurar la eficiencia operacional del diseño del sistema propuesto. Se debieran llevar a cabo las pruebas apropiadas para confirmar que se ha cumplido totalmente con el criterio de aceptación.

Otra información

La aceptación puede incluir un proceso de certificación y acreditación formal para verificar que se hayan tratado apropiadamente los requerimientos de seguridad.

10.4 Protección contra el código malicioso y móvil

Objetivo: Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios debieran estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes debieran introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

10.4.1 Controles contra códigos maliciosos

Control

Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se debieran implementar procedimientos para el apropiado conocimiento del usuario.

Lineamiento de implementación

La protección contra códigos maliciosos se debiera basar en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio. Se debieran considerar los siguientes lineamientos:

a) establecer una política formal prohibiendo el uso de software no-autorizado (ver 15.1.2);
b) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse;
c) realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos comerciales críticos; se debiera investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas;
d) la instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:

1) chequeo de cualquier archivo en medios electrónico u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo;
2) chequear los adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo debiera llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktop y cuando se ingresa a la red de la organización;
3) chequear las páginas Web para detectar códigos maliciosos;

e) definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos (ver 13.1 y 13.2);

f) preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación (ver cláusula 14);

g) implementar procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear Web sites que dan información sobre códigos maliciosos nuevos;

h) implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, los gerentes debieran asegurar que se utilicen fuentes calificadas; por ejemplo, periódicos acreditados, sitios de Internet confiables o proveedores que producen software para protegerse de códigos maliciosos; que diferencien entre bromas pesadas y códigos maliciosos reales; todos los usuarios debieran estar al tanto del problema de las bromas pesadas y qué hacer cuando se reciben.

Otra información

El uso de dos o más productos de software para protegerse de códigos maliciosos a través del ambiente de procesamiento de la información de diferentes vendedores puede mejorar la efectividad de la protección contra códigos maliciosos.

Se puede instalar software para protegerse de códigos maliciosos para proporcionar actualizaciones automáticas de archivos de definición y motores de lectura para asegurarse que la protección esté actualizada. Además, este software se puede instalar en cada desktop para que realice chequeos automáticos.

Se debiera tener cuidado de protegerse contra la introducción de códigos maliciosos durante el mantenimiento y procedimientos de emergencia, los cuales pueden evadir los controles de protección contra códigos maliciosos normales.

10.4.2 Controles contra códigos móviles

Control

Donde se autorice el uso del código móvil, la configuración debiera asegurar que el código móvil autorizado opera de acuerdo con una política de seguridad claramente definida, y se debiera evitar la ejecución del código móvil no-autorizado.

Lineamiento de implementación

Se debieran considerar las siguientes acciones para evitar que el código móvil realice acciones no-autorizadas:

a) ejecutar el código móvil en un ambiente aislado lógicamente;
b) bloquear cualquier uso del código móvil;
c) bloquear lo recibido del código móvil:
d) activar las medidas técnicas conforme estén disponibles en un sistema específico para asegurar el manejo del código móvil;
e) control de los recursos disponibles para el acceso del código móvil;
f) controles criptográficos para autenticar singularmente el código móvil.

Otra información

El código móvil es un código de software que transfiere de una computadora a otra computadora y luego ejecuta automáticamente y realiza un función específica con muy poca o ninguna interacción. El código móvil está asociado con un número de servicios 'middleware'.

Además de asegurar que el código móvil no contenga códigos maliciosos, el control de código móvil es esencial para evitar el uso no-autorizado o interrupción de un sistema o recursos de aplicación y otras fallas en la seguridad de la información.

10.5 Respaldo o Back-Up

Objetivo: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información. Se debieran establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también 14.1) para tomar copias de respaldo de la data y practicar su restauración oportuna.

Control

Se debieran hacer copias de respaldo de la información y software y se debieran probar regularmente en concordancia con la política de copias de respaldo acordada.

Lineamiento de implementación

Se debiera proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se pueda recuperar después de un desastre o falla de medios:

Se debieran considerar los siguientes ítems para el respaldo de la información:

a) se debiera definir el nivel necesario de respaldo de la información;
b) se debieran producir registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración;
c) la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización;
d) las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal;
e) a la información de respaldo se le debiera dar el nivel de protección física y ambiental apropiado (ver cláusula 9) consistente con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo;
f) los medios de respaldo se debieran probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia;
g) los procedimientos de restauración se debieran chequear y probar regularmente para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;
h) en situaciones cuando la confidencialidad es de importancia, las copias de respaldo debieran ser protegidas por medios de una codificación.

Los procedimientos de respaldo para los sistemas individuales debieran ser probados regularmente para asegurar que cumplan con los requerimientos de los planes de continuidad del negocio (ver cláusula 14). Para sistemas críticos, los procedimientos de respaldo debieran abarcar toda la información, aplicaciones y data de todos los sistemas, necesarios para recuperar el sistema completo en caso de un desastre.

Se debiera determinar el período de retención para la información comercial esencial, y también cualquier requerimiento para que las copias de archivo se mantengan permanentemente (ver 15.1.3).

Otra información

Los procedimientos de respaldo pueden ser automatizados para facilitar el proceso de respaldo y restauración. Estas soluciones automatizadas debieran ser probadas suficientemente antes de su implementación y también a intervalos regulares.

10.6 Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de data, implicancias legales, monitoreo y protección. También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

10.6.1 Controles de redes

Control

Las redes debieran ser adecuadamente manejadas y controladas para poder proteger la información en las redes, y mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.

Lineamiento de implementación

Los gerentes de la red debieran implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se debieran considerar los siguientes ítems:

a) cuando sea apropiado, la responsabilidad operacional para las redes se debiera separar de las operaciones de cómputo;
b) se debieran establecer las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario;
c) se debieran establecer controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas; y proyectar los sistemas y aplicaciones conectados (ver 11.4 y 12.3);

también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y las computadoras conectadas;

d) se debiera aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes;

e) las actividades de gestión debieran estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.

Otra información

Se puede encontrar información adicional sobre la seguridad de la red en ISO/IEC 18028, *Tecnología de la Información – Técnicas de seguridad – Seguridad de Red TI*.

10.6.2 Seguridad de los servicios de la red

Control

En todo contrato de redes se debieran identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.

Lineamiento de implementación

Se debiera determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debiera acordar el derecho de auditoría.

Se debieran identificar los acuerdos de seguridad necesarios para servicios particulares; como las características de seguridad, niveles de servicio y requerimientos de gestión. La organización se debiera asegurar que los proveedores de servicio de red implementen estas medidas.

Otra información

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas, redes de valor agregado y soluciones de seguridad de red manejadas como firewalls y sistemas de detección de intrusiones. Estos servicios pueden ir desde una simple banda ancha manejada u ofertas complejas de valor agregado.

Las características de seguridad de los servicios de red pueden ser:

a) la tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red;
b) parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red;
c) cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones.

10.7 Gestión de medios

Objetivo: Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales. Los medios se debieran controlar y proteger físicamente. Se debieran establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), input/output de data y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

10.7.1 Gestión de medios removibles

Control

Debieran existir procedimientos para la gestión de los medios removibles.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para la gestión de medios removibles:

a) si ya no son requeridos, los contenidos de los medios re-usables que no son removidos de la organización no debieran ser recuperables;
b) se debieran establecer los procedimientos para identificar los ítems que podrían requerir de una eliminación segura;
c) podría ser más fácil arreglar que todos los ítems de medios se recolecten y eliminen de forma segura, en lugar de tratar de separar los ítems sensibles o confidenciales;
d) muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipo y medios; se debiera tener cuidado al seleccionar el contratista adecuado con los controles y la experiencia adecuados;
e) cuando sea posible se debiera registrar la eliminación de ítems confidenciales para mantener un rastro de auditoría.

Cuando se acumula medios para ser eliminados, se debiera tener en consideración el efecto de agregación, el cual puede causar que una gran cantidad de información no-confidencial se convierta en confidencial.

Otra información

Se puede divulgar información sensible a través de la eliminación cuidadosa de los medios (ver también 9.2.6 para información sobre la eliminación de equipo).

10.7.3 Procedimientos para el manejo de información

Control

Se debieran establecer los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso.

Lineamiento de implementación

Se debieran establecer los procedimientos para el manipuleo, procesamiento, almacenaje y comunicación de la información consistente con su clasificación (ver 7.2). Se debieran considerar los siguientes ítems:

a) manipuleo y etiquetado de todos los medios en su nivel de clasificación indicado;
b) restricciones de acceso para evitar el acceso de personal no-autorizado;
c) mantenimiento de un registro formal de destinatarios autorizados de la data;
d) asegurar que el input de data esté completo, que el proceso se complete apropiadamente y que se aplique la validación del output;
e) protección de la data recolectada esperando el output en un nivel consistente con la confidencialidad;
f) almacenaje de medios en concordancia con las especificaciones de los fabricantes;
g) mantener la distribución de data en lo mínimo;
h) marcar claramente todas las copias de los medios con atención al destinatario autorizado;
i) revisión de las listas de distribución y las listas de los destinatarios autorizados a intervalos regulares.

Otra información

Estos procedimientos se aplican a la información en documentos; sistemas de cómputo; redes; computación móvil; comunicaciones móviles; comunicaciones vía correo, correo de voz y voz en general; multimedia; servicios/medios postales, uso de máquinas de fax y cualquier otro ítem confidencial; por ejemplo cheques en blanco, facturas.

10.7.4 Seguridad de la documentación del sistema

Control

Se debiera proteger la documentación del sistema con accesos no-autorizados.

Lineamiento de implementación

Para asegurar la documentación del sistema, se debieran considerar los siguientes ítems:

a) la documentación del sistema se debiera almacenar de una manera segura;
b) la lista de acceso para la documentación del sistema se debiera mantener en un nivel mínimo y autorizado por el propietario de la aplicación;
c) la documentación del sistema mantenido en una red pública, o suministrada a través de una red pública, debiera estar adecuadamente protegida.

Otra información

La documentación del sistema puede contener un rango de información confidencial; por ejemplo, una descripción de los procesos de aplicaciones, procedimientos, estructuras de data, procesos de autorización.

10.8 Intercambio de información

Objetivo: Mantener la seguridad en el intercambio de información y software dentro de la organización y con cualquier otra entidad externa. Los intercambios de información y software dentro de las organizaciones se debieran basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (cláusula 15). Se debieran establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en-tránsito.

10.8.1 Políticas y procedimientos de intercambio de información

Control

Se debieran establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.

Lineamiento de implementación

Los procedimientos y controles a seguirse cuando se utilizan medios de comunicación electrónicos para el intercambio de información debieran considerar los siguientes ítems:

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

b) los procedimientos para la detección y protección de contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas (ver Cláusula 10.4.1);

c) los procedimientos para proteger la información electrónica confidencial comunicada que está en la forma de un adjunto;

d) política o lineamientos delineando el uso aceptable de los medios de comunicación electrónicos (ver 7.1.3);

e) los procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados;

f) las responsabilidades del usuario empleado, contratista y cualquier otro para que no comprometan a la organización; por ejemplo, a través de la difamación, hostigamiento, suplantación, reenvío de cadenas de cartas, compras no-autorizadas, etc.

g) uso de técnicas de codificación; por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información (ver Cláusula 12.3);

h) lineamientos de retención y eliminación de toda la correspondencia del negocio, incluyendo mensajes, en concordancia con la legislación y regulaciones nacionales y locales relevantes;

i) no dejar la información confidencial o crítica en medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que personal no-autorizado puede tener acceso a ellas;

j) los controles y restricciones asociados con el reenvío de los medios de comunicación; por ejemplo, reenvío automático de correo electrónico a direcciones externas;

k) recordar al personal que debiera tomar las precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado o interceptado por:

   1) personas alrededor suyo, particularmente cuando se utilizan teléfonos móviles;

   2) intervención de teléfonos y otras formas de escucha no-autorizada a través del acceso físico al teléfono o la línea telefónica, o el uso de escáners receptores;

3) personas en el otro lado de la línea, en el lado del receptor;

l) no dejar mensajes conteniendo información confidencial en máquinas contestadotas dado que estos pueden ser escuchados por personas no-autorizadas, ni almacenados en sistemas comunitarios o almacenados incorrectamente como resultado de un equívoco al marcar;

m) recordar al personal el problema de utilizar máquinas de faz, principalmente por:

1) acceso no autorizado al almacén de mensaje incorporado para recuperar los mensajes;

2) programación deliberada o accidental de las máquinas para enviar mensajes a números específicos;

3) enviar documentos al número equivocado, ya se por marcar un número equivocado o usando un número erróneamente almacenado;

n) recordar al personal no registrar data demográfica, como la dirección de correo electrónico u otra información personal, en ningún software para evitar que sea utilizada sin autorización;

o) recordar al personal que las máquinas de fax y fotocopiadoras modernas tienen páginas cache y almacenan páginas en caso de una falla en la transmisión o papel, las cuales se imprimirán una vez que la falla se aclare.

Además, se debiera recordar al personal que no debieran mantener conversaciones confidenciales en lugares públicos, u oficinas o salas de reuniones abiertas, sin paredes a prueba de ruidos.

Los medios de intercambio de información debieran cumplir con cualquier requerimiento legal relevante (ver cláusula 15).

Otra información

Los intercambios de información pueden ocurrir a través del uso de un número de tipos de comunicación diferentes; incluyendo correo electrónico, de voz, fax y vídeo.

El intercambio de software puede ocurrir a través de un número de medios diferentes; incluyendo la descarga de Internet y el adquirido en una tienda.

Se debieran considerar las implicancias comerciales, legales y de seguridad asociadas con el intercambio electrónico de data, comercio electrónico y comunicaciones electrónicas, y los requerimientos de controles.

La información puede verse comprometida por la falta de conocimiento, política o procedimientos para el uso de los medios de intercambio de información; por ejemplo, ser escuchado al hablar de un teléfono móvil en un lugar público, dirección equivocada en un mensaje de correo electrónico, mensajes dejados en máquinas contestadores escuchados, acceso no-autorizado al sistema de correo de voz o accidentalmente enviar faxes al número equivocado.

Las operaciones comerciales pueden verse interrumpidas y la información puede verse comprometida si fallan los medios de comunicación, son escuchados o interrumpidos (ver 10.3 y la cláusula 14). La información puede verse comprometida si usuarios no-autorizados tienen acceso a ella (ver cláusula 11).

10.8.2 Acuerdos de intercambio

Control

El acuerdo de intercambio debiera considerar las siguientes condiciones de seguridad:

a) manejo de las responsabilidades para el control y notificación de la transmisión, despacho y recepción;
b) procedimientos para notificar al remitente de la transmisión, despacho y recepción;
c) procedimientos para asegurar el rastreo y no-repudio;
d) estándares técnicos mínimos para el empaque y la transmisión;
e) acuerdos de depósitos;
f) estándares de identificación del mensajero;
g) responsabilidades y obligaciones en el evento de incidentes de seguridad de la información, como la pérdida de data;
h) uso de un sistema de etiquetado acordado para la información confidencial o crítica, asegurando que el significado de las etiquetas sea entendido inmediatamente y que la información sea adecuadamente protegida;
i) propiedad y responsabilidades de la protección de data, derechos de autor, licencias de software y consideraciones similares (ver 15.1.2 y 15.1.4);
j) estándares técnicos para grabar y leer la información y software;
k) cualquier control especial que se pueda requerir para proteger los ítems confidenciales, como claves criptográficas (ver 12.3).

Se debieran establecer y mantener las políticas, procedimientos y estándares para proteger la información y medios físicos en tránsito (ver también 10.8.3), y se debiera hacer referencia en los acuerdos de intercambio.

El contenido de seguridad de cualquier acuerdo debiera reflejar la sensibilidad de la información comercial involucrada.

Otra información

Los acuerdos pueden ser electrónicos o manuales, y pueden tomar la forma de contratos formales o condiciones de empleo. Para la información sensible, los mecanismos específicos utilizados para el intercambio de dicha información debieran ser consistente para todas las organizaciones y tipos de acuerdos.

10.8.3 Medios físicos en tránsito

Control

Los medios que contienen información debieran ser protegidos contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para proteger los medios de información transportados entre diferentes ubicaciones:

a) se debieran utilizar transportes o mensajerías confiables;
b) se debiera acordar con la gerencia una lista de mensajerías autorizadas;
c) se debieran desarrollar procedimientos para chequear la identificación de las mensajeros;
d) el empaque debiera ser suficiente para proteger los contenidos de cualquier daño que pudiera surgir durante el tránsito y en concordancia con las especificaciones de cualquier fabricante (por ejemplo, para software), por ejemplo protegiendo de cualquier factor ambiental que pudiera reducir la efectividad de la restauración de medios, tales como la exposición al calor, humedad o campos electromagnéticos;
e) donde sea necesario, se debieran adoptar controles para proteger la información confidencial de la divulgación o modificación no-autorizada, los ejemplos incluyen:
    1) uso de contenedores cerrados con llave;
    2) entrega en la mano;
    3) empaque que haga evidente si ha sido manipulado (el cual revela cualquier intento por obtener acceso);
    4) en casos excepcionales, dividir el envío en más de una entrega y despacharlo por rutas diferentes.

Otra información

La información puede ser vulnerable al acceso no-autorizado, mal uso o corrupción durante el transporte, por ejemplo cuando se envía medios por el servicio postal o servicio de mensajería.

10.8.4 Mensajes electrónicos

Control

Se debiera proteger adecuadamente la información involucrada en mensajes electrónicos.

Lineamiento de implementación

Las consideraciones de seguridad para los mensajes electrónicos debieran incluir lo siguiente:

a) proteger los mensajes del acceso no-autorizado, modificación o negación del servicio;
b) asegurar la correcta dirección y transporte del mensaje;
c) confiabilidad y disponibilidad general del servicio;
d) consideraciones legales, por ejemplo los requerimientos para firmas electrónicas;
e) obtener la aprobación antes de utilizar los servicios públicos externos como un mensaje instantáneo o intercambio de archivos;
f) niveles mayores de autenticación controlando el acceso de las redes de acceso público.

Otra información

Los mensajes electrónicos como el correo electrónico, Intercambio Electrónico de Data (EDI), y los mensaje instantáneos representa un papel cada vez más importante en las comunicaciones comerciales. Los mensajes electrónicos tienen riesgos diferentes que las comunicaciones basadas en papel.

10.8.5 Sistemas de información comercial

Control

Se debieran desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.

Lineamiento de implementación

La consideración dada a las implicancias de seguridad y comerciales de interconectar dichos medios debiera incluir:

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

b) las vulnerabilidades de la información en los sistemas de comunicación comercial; por ejemplo, grabando llamadas o conferencias telefónicas, la confidencialidad de las llamadas, almacenaje de faxes, apertura de correo, distribución del correo;

c) política y los controles apropiados para manejar el intercambio de información;

d) excluir las categorías de información comercial confidencial y los documentos clasificados si el sistema no proporciona un nivel de protección apropiado (ver 7.2);

e) restringir el acceso a la información diaria relacionada con personas seleccionadas; por ejemplo, el personal trabajando en proyectos confidenciales;

f) categorías del personal, contratistas o socios comerciales con autorización para utilizar el sistema y las ubicaciones desde las cuales pueden tener acceso (ver 6.2 y 6.3);

g) restringir los medios seleccionados a categorías de usuarios específicas;

h) identificar el status de los usuarios; por ejemplo, los empleados de la organización o contratistas en directorios para beneficio de otros usuarios;

i) retención y respaldo de la información mantenida en el sistema (ver 10.5.1);

j) requerimientos y acuerdos alternativos (ver 14).

Otra información

Los sistemas de información de oficina son oportunidades para una difusión e intercambio más rápidos de la información comercial utilizando una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios/medios postales y máquinas de fax.

10. 9 Servicios de comercio electrónico

Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro. Se debieran considerar las implicancias de seguridad asociadas con el uso de servicios de comercio electrónico, incluyendo las transacciones en-línea, y los requerimientos de controles. También se debieran considerar la integridad y la disponibilidad de la información publicada electrónicamente a través de los sistemas públicamente disponibles.

10.9.1 Comercio electrónico

Control

La información involucrada en el comercio electrónico que pasa a través de redes públicas debiera protegerse de la actividad fraudulenta, disputas de contratos, divulgación no-autorizada y modificación.

Lineamiento de implementación

Las consideraciones de seguridad para el comercio electrónico debieran incluir lo siguiente:

a) el nivel de confianza que cada parte requiere de la identidad de la otra; por ejemplo, a través de la autenticación;
b) los procesos de autorización asociados con aquellos que pueden establecer precios, emitir o firmar documentos de comercialización;
c) asegurar que los socios comerciales estén totalmente informados de sus autorizaciones;
d) determinar y cumplir con los requerimientos para la confidencialidad, integridad, prueba de despacho y recepción de documentos claves, y el no-repudio de los contratos; por ejemplo, asociado con procesos de licitación y contratos;
e) el nivel de confianza requerido para la integridad de las listas de precios publicitadas;
f) la confidencialidad de cualquier data o información confidencial;
g) la confidencialidad e integridad de cualquier transacción, información de pago, detalles de la dirección de entrega y la confirmación de la recepción;
h) el grado de verificación apropiado para chequear la información de pago suministrada por un cliente;
i) seleccionar la forma de liquidación más apropiada del pago para evitar el fraude;
j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de la orden;
k) evitar la pérdida o duplicación de la información de la transacción;
l) la responsabilidad asociada con cualquier transacción fraudulenta;
m) requerimientos de seguro.

Muchas de las consideraciones arriba mencionadas se pueden tratar mediante la aplicación de controles criptográficos (ver 12.3), tomando en cuenta el cumplimiento de los requerimientos legales (ver 15.1, especialmente 15.1.6 para la legislación criptográfica).

Los acuerdos de comercio electrónico entre socios debieran ser respaldados por un contrato documentado el cual compromete a ambas partes a los términos acordados para la comercialización, incluyendo los detalles de la autorización (ver b) arriba). Pueden ser necesarios otros acuerdos con los proveedores del servicio de la información y la red de valor agregado.

Los sistemas de negociación pública debieran comunicar sus términos del negocio a sus clientes.

Se debiera tomar en consideración a la resistencia al ataque del host(s) utilizado(s) para el comercio electrónico, y las implicancias de seguridad de cualquier interconexión de la red requerida para la implementación de los servicios de comercio electrónico (ver 11.4.6).

Otra información

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

El comercio electrónico puede utilizar métodos de autenticación; por ejemplo, criptografía clave pública y firmas electrónicas (ver también 12.3) para reducir los riesgos. También, se pueden utilizar terceros confiables cuando se necesitan dichos servicios.

10.9.2 Transacciones en-línea

Control

Se debiera proteger la información involucrada en las transacciones en-línea para evitar una transmisión incompleta, routing equivocado, alteración no-autorizada del mensaje, divulgación no-autorizada, duplicación o repetición no-autorizada del mensaje.

Lineamiento de implementación

Las consideraciones de seguridad para las transacciones en-línea debieran incluir lo siguiente:

c) el uso de firmas electrónicas por cada una de las partes involucradas en la transacción;
d) todos los aspectos de la transacción; es decir, asegurando que:
    1) las credenciales de usuario de todas las partes sean válidas y verificadas;
    2) que la transacción permanezca confidencial; y
    3) que se mantenga la privacidad asociada con todas las partes involucradas;
e) el camino de las comunicaciones entre las partes involucradas debiera ser codificado;
f) los protocolos utilizados para comunicarse entre todas las partes involucradas sean seguros;
g) asegurar que el almacenaje de los detalle de la transacción se localice fuera de cualquier ambiente público accesible; por ejemplo, en una plataforma de almacenaje existente en el Intranet organizacional, y no se mantenga y exponga en un medio de almacenaje directamente accesible desde el Internet;
h) cuando se utilice una autoridad confiables (por ejemplo, para propósitos de emitir y mantener firmas digitales y/o certificados digitales) la seguridad es integrada e introducida durante todo el proceso de gestión de firma/certificado de principio a fin.

Otra información

La extensión de los controles adoptados debiera conmensurarse con el nivel del riesgo asociado con cada forma de transacción en-línea.

Las transacciones pueden necesitar cumplir con leyes, reglas y regulaciones en la jurisdicción en la cual se genera, procesa, completa y/o almacena la transacción.

Existen muchas formas de transacciones que se pueden realizar de una manera en-línea; por ejemplo, contractuales, financieras, etc.

10.9.3 Información públicamente disponible

Control

Se debiera proteger la integridad de la información puesta a disposición en un sistema públicamente disponible para evitar una modificación no-autorizada.

Lineamiento de implementación

El software, data y otra información que requiere un alto nivel de integridad, puesta a disposición en un sistema públicamente disponible, se debiera proteger mediante los mecanismos apropiados; por ejemplo, firmas digitales (ver 12.3). El sistema públicamente disponible debiera ser probado en busca de debilidades y fallas antes que la información esté disponible.

Debiera existir un proceso de aprobación formal antes que la información sea puesta a disposición pública. Además, se debiera verificar y aprobar todo el input provisto desde fuera del sistema.

Se debieran controlar cuidadosamente los sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y el ingreso directo de información de manera que:

a) la información se obtenga cumpliendo con la legislación de protección de data (ver 15.1.4);
b) el input de información para, y procesado por, el sistema de publicación será procesado completa y exactamente de una manera oportuna:
c) se protegerá la información confidencial durante la recolección, procesamiento y almacenaje;
d) el acceso al sistema de publicación no permite el acceso involuntario a las redes con las cuales se conecta el sistema.

Otra información

La información en un sistema públicamente disponible; por ejemplo, información en un servidor Web accesible vía Internet; puede necesitar cumplir con las leyes, reglas y regulaciones en la jurisdicción en la cual se ubica el sistema, donde se realiza el negocio o donde reside(n) el(los) propietario(s). La modificación no-autorizada de la información publicada puede dañar la reputación de la organización editora.

10.10 Monitoreo

Objetivo: Detectar las actividades de procesamiento de información no autorizadas.
Se debieran monitorear los sistemas y se debieran reportar los eventos de seguridad de la información. Se debieran utilizar bitácoras de operador y se debieran registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información.
Una organización debiera cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.
Se debiera utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

10.10.1 Registro de auditoría

Control

Se debieran producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

Lineamiento de implementación

Los registros de auditoría debieran incluir, cuando sea relevante:

a) utilizar IDs;
b) fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida;
c) identidad o ubicación de la identidad, si es posible;
d) registros de intentos de acceso fallidos y rechazados al sistema;
e) registros de intentos de acceso fallidos y rechazados a la data y otros recursos;
f) cambios en la configuración del sistema;
g) uso de privilegios;
h) uso de las utilidades y aplicaciones del sistema;

i) archivos a los cuales se tuvo acceso y los tipos de acceso;

j) direcciones y protocolos de la red;

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

l) activación y desactivación de los sistemas de protección; como sistemas anti-virus y sistemas de detección de intrusiones.

Otra información

Los registros de auditoría pueden contener data personal confidencial. Se debieran mantener las medidas de protección de privacidad apropiadas (ver también 15.1.4). Cuando sea posible, los administradores del sistema no debieran tener permiso para borrar o desactivar los registros de sus propias actividades (ver 10.1.3).

10.10.2 Uso del sistema de monitoreo

Control

Se debieran establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se debieran revisar regularmente los resultados de las actividades de monitoreo.

Lineamiento de la implementación

Se debiera determinar el nivel de monitoreo requerido para los medios individuales mediante una evaluación del riesgo. Una organización debiera cumplir con los requerimientos legales relevantes aplicables para sus actividades de monitoreo. Las áreas que se debieran considerar incluyen:

a) acceso autorizado, incluyendo detalles tales como:
    1) ID del usuario;
    2) fecha y hora de los eventos claves;
    3) tipos de eventos;
    4) archivo a los cuales se tuvo acceso;
    5) programas/utilidades utilizados;

b) todas las operaciones privilegiadas, tales como:
    1) uso de las cuentas privilegiadas; por ejemplo, supervisor, raíz,, administrador,
    2) inicio y apagado del sistema;
    3) dispositivo I/O para adjuntar y eliminar lo adjuntado;´

c) intentos de acceso no autorizado, como:
    1) accesiones del usuario fallidas o rechazadas;
    2) acciones fallidas o rechazadas que involucran la data y otros recursos;

3) violaciones a la política de acceso y notificaciones para los 'gateways' y 'firewalls' de la red;
4) alertas de los sistemas de detección de intrusiones;

d) alertas o fallas del sistema como:

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

d) cambios o intentos de cambio en los marcos y controles del sistema de seguridad.

La frecuencia con que se revisan los resultados de las actividades de monitoreo dependerá de los riesgos involucrados. Los factores de riesgo a considerarse incluyen:

a) grado crítico de los procesos de aplicación;
b) valor, sensibilidad y grado crítico de la información involucrada;
c) antecedentes de infiltración y mal uso del sistema, y la frecuencia con la que se explotan las vulnerabilidades;
d) extensión de la interconexión del sistema (particularmente las redes públicas);
e) desactivación del medio de registro.

Otra información

Es necesaria la utilización de procedimientos de monitoreo para asegurar que los usuarios sólo estén realizando actividades para las cuales han sido explícitamente autorizados.

La revisión del registro involucra entender las amenazas que enfrenta el sistema, y la manera en que estas surgen. En 13.1.1 se proporcionan ejemplos de eventos que podrían requerir mayor investigación en caso de incidentes en la seguridad de la información.

10.10.3 Protección del registro de información

Control

Se debieran proteger los medios de registro y la información del registro para evitar la alteración y el acceso no autorizado.

Lineamiento de implementación

Los controles debieran tener el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro debiera incluir:

a) las alteraciones registradas a los tipos de mensajes;
b) los archivos de registro que se editan o borran;

c) capacidad de almacenamiento del medio de archivos de registro que se está excediendo, resultando en una falla en el registro de eventos o la escritura encima de los eventos registrados en el pasado.

Se pueden requerir archivar los registros de auditoría como parte de la política de retención de archivos o debido a los requerimientos para recolectar y mantener evidencia (ver también 13.2.3).

Otra información

Los registros del sistema con frecuencia contienen un gran volumen de información, gran parte del cual no relacionado con el monitoreo de seguridad. Para ayudar a identificar los eventos significativos para propósitos del monitoreo de seguridad, se puede considerar el copiado automático de los tipos de mensajes apropiados a un segundo registro, y/o el uso de utilidades del sistema o herramientas de auditoría adecuadas para realizar la interrogación y racionalización del archivo.

Se necesita proteger los registros del sistema, porque si la data puede ser modificada o se puede borrar la data en ellos, su existencia puede crear un falso sentido de seguridad.

10.10 4 Registros del administrador y operador

Control

Se debieran registrar las actividades del administrador del sistema y el operador del sistema.

Lineamiento de implementación

Los registros debieran incluir:

a) la hora en la cual ocurre un evento (éxito o falla);
b) la información sobre el evento (por ejemplo, archivos manejados) o falla (por ejemplo, el error ocurrido y la acción correctiva);
c) cuál cuenta y cuál operador o administrador está involucrado;
d) cuáles procesos están involucrados.

Los registros de administrador y operador del sistema debieran ser revisados de manera regular.

Otra información

Se puede utilizar un sistema de detección de intrusiones manejado fuera del control del sistema y los administradores del sistema para monitorear el sistema y las actividades de administración de la red para chequear su cumplimiento.

10.10.5 Registro de fallas

Control

Se debieran registrar y analizar las fallas, y se debieran tomar las acciones necesarias.

Lineamiento de implementación

Se debieran registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con los problemas con el procesamiento de la información o los sistemas de comunicación. Debieran existir reglas claras para manejar las fallas reportadas incluyendo:

a) revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente;
b) revisión de las medidas correctivas para asegurar que los controles no se hayan visto comprometidos, y que la acción tomada haya sido completamente autorizada.

Se debiera asegurar que el registro de errores está activado, si está disponible esta función del sistema.

Otra información

Los registros de errores y fallas pueden tener un impacto en el desempeño del sistema. Este registro debiera ser facilitado por el personal competente, y se debiera determinar el nivel de registro requerido para los sistemas individuales mediante una evaluación del riesgo, tomando en cuenta la degradación del desempeño.

10.10.6 Sincronización de relojes

Control

Los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se debieran sincronizar con una fuente que proporcione la hora exacta acordada.

Lineamiento de implementación

Cuando una computadora o dispositivo de comunicaciones tiene la capacidad para operar un reloj de tiempo-real, este reloj debiera ser puesto a la hora de acuerdo a un estándar acordado; por ejemplo, el Tiempo Universal Coordinado (UTC) o la hora estándar local. Ya

que algunos relojes se atrasan o adelantan a lo largo del tiempo, debiera existir un procedimiento que los chequee y corrija cualquier variación significativa.

La correcta interpretación de un formato fecha/hora es importante para asegurar que el sello de fecha/hora refleje la fecha/hora real. Se debieran tomar en cuenta las especificaciones locales (por ejemplo, ahorro por luz solar).

Otra información

El ajuste correcto de los relojes del computador es importante para asegurar la exactitud de los registros de auditoría, los cuales se pueden requerir para investigaciones o como evidencia en casos legales o disciplinarios. Registros de auditoría inexactos pueden entorpecer estas investigaciones y dañar la credibilidad de tales evidencias. Se puede utilizar un reloj vinculado con la difusión de la hora de un reloj atómico nacional como reloj maestro para los registros de los sistemas. Se puede utilizar un protocolo de hora de red para mantener todos los servidores sincronizados con el reloj maestro.

Control del acceso

11.1 Requerimiento del negocio para el control del acceso

Objetivo: Controlar el acceso a la información. Se debiera controlar el acceso a la información, medios de procesamiento de la información y procesos comerciales sobre la base de los requerimientos comerciales y de seguridad. Las reglas de control del acceso debieran tomar en cuenta las políticas para la divulgación y autorización de la información.

11.1.1 Política de control del acceso

Control

Se debiera establecer, documentar y revisar la política de control de acceso en base a los requerimientos comerciales y de seguridad para el acceso.

Lineamiento de implementación

Las reglas de control del acceso y los derechos para cada usuario o grupos de usuarios se debieran establecer claramente en la política de control de acceso. Los controles de acceso son tanto lógicos como físicos (ver también la sección 9) y estos debieran ser considerados

juntos. Se debiera proporcionar a los usuarios y proveedores del servicio un enunciado claro de los requerimientos comerciales que debieran cumplir los controles de acceso.

La política debiera tomar en cuenta lo siguiente:

a) los requerimientos de seguridad de las aplicaciones comerciales individuales;
b) identificación de toda la información relacionada con las aplicaciones comerciales y los riesgos que enfrenta la información;
c) las políticas para la divulgación y autorización de la información; por ejemplo, la necesidad de conocer el principio y los niveles de seguridad, y la clasificación de la información (ver 7.2);
d) consistencia entre el control del acceso y las políticas de clasificación de la información de los diferentes sistemas y redes;
e) legislación relevante y cualquier obligación contractual relacionada con la protección del acceso a la data o los servicios (ver 15.1);
f) los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización;
g) gestión de los derechos de acceso en un ambiente distribuido y en red que reconoce todos los tipos de conexiones disponibles;
h) segregación de roles del control del acceso; por ejemplo, solicitud de acceso, autorización de acceso, administración del acceso;
i) requerimientos para la autorización formal de las solicitudes de acceso;
j) requerimientos para la revisión periódica de los controles de acceso (ver 11.2.4);
k) revocación de los derechos de acceso (ver 8.3.3).

Otra información

Se debiera tener cuidado cuando se especifican los controles de acceso para considerar:

a) la diferenciación entre las reglas que siempre se debieran seguir y los lineamientos que son opcionales o condicionales;
b) establecer reglas basadas en la premisa “Generalmente todo está prohibido a no ser que esté expresamente permitido” en lugar de la regla más débil, “Generalmente todo está permitido a no ser que esté expresamente prohibido”;
c) cambios en las etiquetas de la información (ver 7.2) que son iniciados automáticamente por los medios de procesamiento de la información y aquellos iniciados por un administrador;
d) cambios en los permisos del usuario que son iniciados automáticamente por el sistema de información y aquellos iniciados por el administrador;
e) reglas que requieren aprobación específica antes de ser promulgadas, y aquellas que no.

Las reglas de control del acceso debieran ser respaldadas por procedimientos formales y responsabilidades claramente definidas (ver, por ejemplo, 6.13, 11.3, 10.4.1, 11.6).

11.2 Gestión de acceso del usuario

Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información Se debieran establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información. Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta el des-registro final de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Cuando sea apropiado, se debiera prestar atención especial a la necesidad de controlar la asignación de derechos de acceso privilegiados, lo que permite a los usuarios superar los controles del sistema.

11.2.1 Registro del usuario

Control

Debiera existir un procedimiento formal para el registro y des-registro del usuario para otorgar y revocar el acceso a todos los sistemas y servicios de información.

Lineamiento de implementación

El procedimiento de control del acceso para el registro y des-registro del usuario debiera incluir:

a) utilizar IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones; sólo se debiera permitir el uso de IDs grupales cuando son necesarios por razones comerciales u operacionales, y debieran ser aprobados y documentados;

b) chequear que el usuario tenga la autorización dada por el propietario del sistema para el uso del sistema o servicio de información; también puede ser apropiado una aprobación separada de la gerencia para los derechos de acceso;

c) chequear que el nivel de acceso otorgado sea apropiado para el propósito comercial (ver 11.1) y que sea consistente con la política de seguridad de la organización; por ejemplo, no compromete la segregación de los debierares (ver 10.1.3);

d) proporcionar a los usuarios un enunciado escrito de sus derechos de acceso;

e) requerir a los usuarios que firmen los enunciados indicando que entienden las condiciones de acceso;
f) asegurar que los proveedores del servicio no proporcionen acceso hasta que se hayan completado los procedimientos de autorización;
g) mantener un registro formal de todas las personas registradas para usar el servicio;
h) eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo o han dejado la organización;
i) chequeo periódico para eliminar o bloquear los IDs de usuario y cuentas redundantes (ver 11.2.4);
j) asegurar que no se emitan IDs de usuario redundantes a otros usuarios.

Otra información

Se debiera considerar establecer roles de acceso de usuarios basados en los requerimientos que resuman un número de derechos de acceso en perfiles de acceso de usuario típicos. Las solicitudes y revisiones del acceso (ver 11.2.4) son más fáciles de manejar en el nivel de dichos roles en lugar de en el nivel de derechos particulares.

Se debiera considerar incluir en los contratos del personal y contratos de servicio cláusulas que especifiquen las sanciones si el personal o los agentes de servicio intentan un acceso no autorizado (ver también 6.1.5, 8.1.3 y 8.2.3).

11.2.2 Gestión de privilegios

Control

Se debiera restringir y controlar la asignación y uso de privilegios.

Lineamiento de implementación

Los sistemas multi-usuario que requieren protección contra el acceso no autorizado debieran controlar la asignación de privilegios a través de un proceso de autorización formal. Se debieran considerar los siguientes pasos:

a) los privilegios de acceso asociados con cada producto del sistema; por ejemplo, sistema de operación, sistema de gestión de base de datos y cada aplicación, y se debieran identificar los usuarios a quienes se les necesita asignar privilegios;
b) los privilegios se debieran asignar a los usuarios sobre la base de "sólo lo que necesitan saber" y sobre una base de evento-por-evento en línea con la política de control del acceso (11.1.1); es decir, los requerimientos mínimos para su rol funcional, sólo cuando se necesitan;

c) se debiera mantener un proceso de autorización y un registro de todos los privilegios asignados. No se debieran otorgar privilegios hasta que se complete el proceso de autorización.

d) Se debiera promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios;

e) se debiera promover el desarrollo y uso de los programas que evitan la necesidad de correr con privilegios;

f) los privilegios se debieran asignar a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio.

Otra información

El uso inapropiado de los privilegios de administración del sistema (cualquier dispositivo o medio de un sistema de información que permite al usuario superar los controles del sistema o aplicación) puede ser un factor que contribuye mucho a las fallas o violaciones del sistema.

11.2.3 Gestión de las claves secretas de los usuarios

Control

La asignación de claves secretas se debiera controlar a través de un proceso de gestión formal.

Lineamiento de implementación

El proceso debiera incluir los siguientes requerimientos:

a) se debiera requerir que los usuarios firmen un enunciado para mantener confidenciales las claves secretas y mantener las claves secretas grupales sólo dentro de los miembros el grupo; este enunciado firmado se puede incluir en los términos y condiciones de empleo (ver 8.1.3);

b) cuando se requiere que los usuarios mantengan sus propias claves secretas, inicialmente se les debiera proporcionar una clave secreta temporal segura (ver 11.3.1), la cual están obligados a cambiar inmediatamente;

c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nuevo, sustituta o temporal;

d) las claves secretas temporales debieran ser proporcionadas a los usuarios de una manera segura, se debiera evitar el uso de mensajes de correo electrónico de terceros o no protegidos (sin texto);

e) las claves secretas temporales debieran ser únicas para la persona y no debieran ser fáciles de adivinar;

f) los usuarios debieran reconocer la recepción de las claves secretas;

g) las claves secretas nunca debieran ser almacenadas en los sistemas de cómputo de una forma desprotegida;

h) las claves secretas predeterminadas por el vendedor debieran ser cambiadas después de la instalación de sistemas o software.

Otra información

Las claves secretas son un medio común para verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de información en concordancia con la autorización del usuario. Están disponibles, y se debiera considerar la idoneidad, de otras tecnologías para la identificación y autenticación del usuario; tales como biométricas, por ejemplo verificación de huellas digitales, verificación de firmas; y el uso de dispositivos de hardware como tarjetas inteligentes.

11.2.4 Revisión de los derechos de acceso del usuario

Control

La gerencia debiera revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.

Lineamiento de implementación

La revisión de los derechos de acceso debiera considerar los siguientes lineamientos:

a) los derechos de acceso de los usuarios debieran ser revisados a intervalos regulares; por ejemplo, un período de 6 meses, y después de cualquier cambio, como un ascenso, democión o terminación del empleo (ver 11.2.1);

b) los derechos de acceso del usuario se debieran revisar y re-asignar cuando se traslada de un empleo a otro dentro de la misma organización;

c) las autorizaciones para derechos de acceso privilegiados especiales (ver 11.2.2) se debieran revisar a intervalos más frecuentes; por ejemplo, un período de 3 meses;

d) se debiera chequear la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados;

e) se debieran registrar los cambios en las cuentas privilegiadas para una revisión periódica.

Otra información

Es necesario revisar regularmente los derechos de acceso de los usuarios para mantener un control efectivo sobre el acceso a la data y los servicios de información.

11.3 Responsabilidades del usuario

Objetivo: Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información. La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios debieran estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario. Se debiera implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

11.3.1 Uso de claves secretas

Control

Se debiera requerir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de claves secretas.

Lineamiento de implementación

Se debiera advertir a todos los usuarios que:

a) mantener confidenciales las claves secretas;
b) evitar mantener un registro (por ejemplo, papel, archivo en software o dispositivo manual) de las claves secretas, a no ser que este se pueda mantener almacenado de manera segura y el método de almacenaje haya sido aprobado;
c) cambio de claves secretas cuando haya el menor indicio de un posible peligro en el sistema o la clave secreta;
d) seleccionar claves secretas de calidad con el largo mínimo suficiente que sean:
    1) fáciles de recordar;
    2) no se basen en nada que otro pueda adivinar fácilmente u obtener utilizando la información relacionada con la persona; por ejemplo, nombres, números telefónicos y fechas de nacimiento, etc.
    3) no sean vulnerables a los ataques de diccionarios (es decir, que no consista de palabras incluidas en los diccionarios);
    4) libre de caracteres consecutivos idénticos, todos numéricos o todos alfabéticos;
e) cambio de las claves secretas a intervalos regulares o en base al número de accesos (las claves secretas para las cuentas privilegiadas se debieran cambiar con mayor

frecuencia que las claves secretas normales), y evitar el re-uso de reciclaje de claves secretas antiguas;

f) cambiar la clave secreta temporal en el primer registro de ingreso;
g) no incluir las claves secretas en ningún proceso de registro automatizado; por ejemplo, almacenado en un macro o función clave;
h) no compartir las claves secretas individuales;
i) no usar la misma clave personal para propósitos comerciales y no-comerciales

Si los usuarios necesitan tener acceso a múltiples servicios, sistemas o plataformas, y requieren mantener múltiples claves secretas separadas, se les debiera advertir que pueden utilizar una sola clave secreta de calidad (ver d) en el párrafo anterior) para todos los servicios donde se le asegura al usuario que se ha establecido un nivel de protección razonable para el almacenaje de la clave secreta dentro de cada servicio, sistema o plataforma.

Otra información

Se necesita tener especial cuidado con el manejo del sistema de 'help desk' para las claves secretas perdidas u olvidadas ya que este también puede ser un medio para atacar al sistema de clave secretas.

11.3.2 Equipo del usuario desatendido

Control

Los usuarios debieran asegurar que el equipo desatendido tenga la protección apropiada.

Lineamiento de implementación

Todos los usuarios debieran estar al tanto de los requerimientos de seguridad y los procedimientos para proteger el equipo desatendido, así como sus responsabilidades para implementar dicha protección. Se debiera comunicar a los usuarios que debieran:

a) cerrar las sesiones activas cuando se termina, a no ser que puedan asegurarse con un mecanismo de cierre apropiado; por ejemplo, protector de pantalla asegurado mediante clave secreta;
b) salir de las computadoras mainframe, servidores y PCs de oficina cuando se termina la sesión (es decir, no sólo apagar la pantalla de la PC o Terminal);
c) asegurar las PCs o terminales contra un uso no autorizado mediante un seguro con clave o un control equivalente; por ejemplo, acceso con clave secreta, cuando no está en uso (ver también 11.3.3).

Otra información

El equipo instalado en las áreas de usuarios; por ejemplo estaciones de trabajo o servidores de archivo; puede requerir protección específica contra el acceso no autorizado cuando se deja desatendido durante un período e tiempo extendido.

11.3.3 Política de escritorio y pantalla limpios

Control

Se debiera adoptar una política de escritorio limpio para papeles y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.

Lineamiento de implementación

La políticas de escritorio limpio y pantalla limpia debieran tomar en cuenta las clasificaciones de información (ver 7.2), requerimientos legales y contractuales (ver 15.1), y los correspondientes riesgos y aspectos culturales de la organización. Se debieran considerar los siguientes lineamientos:

a) la información comercial confidencial o crítica; por ejemplo, en papel o medios de almacenamiento electrónicos; debiera ser guardada bajo llave (idealmente en una caja fuerte o archivador u otra forma de mueble seguro) cuando no está siendo utilizada, especialmente cuando la oficina está vacía;

b) cuando se dejan desatendidas, las computadoras y terminales debieran dejarse apagadas o protegidas con mecanismos para asegurar la pantalla y el teclado, controlados mediante una clave secreta, dispositivo o un mecanismo de autenticación de usuario similar y se debieran proteger con llave, claves secretas u otros controles cuando no están en uso;

c) se debieran proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidas;

d) se debiera evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáners, cámaras digitales);

e) los documentos que contienen información confidencial o clasificada debieran sacarse inmediatamente de la impresora.

Otra información

Una política de escritorio/pantalla limpia reduce el riesgo de accesos no-autorizados, pérdida y daño a la información durante y fuera el horario de trabajo normal. Los seguros u otras formas de medios de almacenaje seguro también podrían proteger la información almacenada contra desastres como fuego, terremotos, inundaciones o explosiones.

Considere el uso de impresoras con la función de clave secreta, de manera que sólo los creadores de un documento puedan imprimirlo, y sólo cuando estén parados junto a la impresora.

11.4 Control de acceso a la red

Objetivo: Evitar el acceso no autorizado a los servicios de la red. Se debiera controlar el acceso a los servicios de redes internas y externas. El acceso del usuario a las redes y servicios de las redes no debieran comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfases apropiadas entre la red de la organización y las redes de otras organizaciones, y redes públicas; b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo; c) el control del acceso del usuario a la información sea obligatorio.

11.4.1 Política sobre el uso de los servicios de la red

Control

Los usuarios sólo debieran tener acceso a los servicios para los cuales hayan sido específicamente autorizados.

Lineamiento de implementación

Se debiera formular una política relacionada con el uso de las redes y los servicios de la red. Esta política debiera abarcar:

a) las redes y servicios de la red a las cuales se tiene acceso;
b) los procedimientos de autorización para determinar quién está autorizado a tener acceso a cuáles redes y servicios en red;
c) controles y procedimientos gerenciales para proteger el acceso a las conexiones de la red y los servicios en red;
d) los medios utilizados para tener acceso a las redes y los servicios de la red (por ejemplo, las condiciones para permitir acceso vía discado a un proveedor del servicio de Internet o sistema remoto).

La política sobre el uso de los servicios de la red debiera ser consistente con la política de control de acceso del negocio (ver 11.1)

Otra información

Las conexiones no autorizadas e inseguras a los servicios de la red pueden afectar a toda la organización. Este control es particularmente importante para las conexiones de la red con aplicaciones comerciales confidenciales o críticas o con usuarios en ubicaciones de alto riesgo; por ejemplo, áreas públicas o externas que están fuera de la gestión y control de seguridad de la organización.

11.4.2 Autenticación del usuario para las conexiones externas

Control

Se debieran utilizar métodos de autenticación apropiados para controlar el acceso de usuarios remotos.

Lineamiento de implementación

La autenticación de los usuarios remotos se puede lograr utilizando, por ejemplo, una técnica basada en criptografía, dispositivos de hardware o un protocolo de desafío/respuesta. Las posibles implementaciones de tales técnicas se pueden encontrar en varias soluciones de la red privada virtual (VPN). También se pueden utilizar las líneas privadas dedicadas para proporcionar la seguridad de la fuente de conexiones.

Los procedimientos y controles de discado; por ejemplo, utilizando módems de discado; pueden proporcionar protección contra conexiones no autorizadas e indeseadas a los medios de procesamiento de la información de una organización. Este tipo de control ayuda a autenticar a los usuarios que tratan de establecer una conexión con la red de la organización desde ubicaciones remotas. Cuando se utiliza este control, una organización no debiera utilizar los servicios de red, los cuales incluyen reenvío de llamadas, y si lo hacen, debieran deshabilitar el uso de tales dispositivos para evitar las debilidades asociadas con el reenvío de llamadas. El proceso de llamada de verificación debieraría asegurar que ocurra una desconexión real en el lado de la organización. De otra manera, el usuario remoto podría tomar la línea abierta pretendiendo que ha ocurrido la llamada de verificación. Los procedimientos y controles de la llamada de verificación debieran ser comprobados concienzudamente para evitar esta posibilidad.

La autenticación del nodo puede servir como un medio alternativo para la autenticación de los grupos de usuarios remotos, cuando están conectados a un medio de cómputo seguro y compartido. Se pueden utilizar técnicas criptográficas; por ejemplo, basadas en los certificados de las máquinas; para la autenticación del nodo.

Se debieran implementar controles de autenticación adicionales para controlar el acceso a las redes inalámbricas. En particular, se necesita prestar cuidado especial a la selección de controles para las redes inalámbricas debido a las mayores oportunidades para una intercepción e inserción no-detectada de tráfico de la red.

Otra información

Las conexiones externas proporcionan un potencial para el acceso no autorizado a la información comercial; por ejemplo, acceso mediante métodos de discado. Existen diferentes tipos de métodos de autenticación, algunos de estos proporcionan un mayor nivel de protección que otros; por ejemplo, los métodos basados en el uso de las técnicas criptográficas pueden proporcionar una autenticación sólida. Es importante determinar el nivel de protección requerido mediante una evaluación del riesgo. Esto es necesario ara la selección apropiada de un método de autenticación.

Un medio para la conexión automática con una computadora remota podría proporcionar una manera de obtener acceso no autorizado a la aplicación comercial. Esto es especialmente importante si la conexión utiliza una red que esté fuera del control de la gestión de seguridad de la organización.

11.4.3 Identificación del equipo en las redes

Control

La identificación automática del equipo se debiera considerar como un medio para autenticar las conexiones de ubicaciones y equipos específicos.

Lineamiento de implementación

La identificación del equipo se puede utilizar si es importante que la comunicación sólo sea iniciada desde una ubicación o equipo específico. Se puede utilizar un identificador dentro o incorporado en el equipo para indicar si este equipo está autorizado a conectarse a la red. Estos identificadores debieran indicar claramente a cuál red está autorizado a conectarse el equipo, si existe más de una red y particularmente si estas redes tienen diferentes grados de confidencialidad. Puede ser necesario considerar la protección física del equipo para mantener la seguridad del identificador del equipo.

Otra información

Este control puede complementarse con otras técnicas para autenticar al usuario del equipo (ver 11.4.2). Adicionalmente, se puede aplicar la identificación del equipo para la autenticación del usuario.

11.4. Protección del puerto de diagnóstico y configuración remoto

Control

Se debiera controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.

Lineamiento de implementación

Los controles potenciales para el acceso a los puertos de diagnostico y configuración incluyen el uso de un seguro y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es asegurar que los puertos de diagnóstico y configuración sólo sean accesibles a través de un acuerdo entre el gerente del servicio de cómputo y el personal de soporte de hardware/software que requiere acceso.

Los puertos, servicios y medios similares instalados en una computadora o red, que no son requeridos específicamente por funcionalidad comercial, debieran ser desactivados o removidos.

Otra información

Muchos sistemas de cómputo, sistemas de redes y sistemas de comunicaciones están instalados con un medio de diagnóstico o configuración remoto para ser utilizado por los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado.

11.4.5 Segregación en redes

Control

Los grupos de servicios de información, usuarios y sistemas de información debieran ser segregados en redes.

Lineamiento de implementación

Un método para controlar la seguridad de grandes redes es dividirlas en dominios de red lógicos separados; por ejemplo, dominios de red internos y dominios de red externos de una organización; cada uno protegido por un perímetro de seguridad definido. Se puede aplicar un conjunto de controles graduados en dominios de red lógicos diferentes para segregar aún más los ambientes de seguridad de la red; por ejemplo, sistemas de acceso público, redes internas

y activos críticos. Los dominios debieran ser definidos en base a una evaluación del riesgo y los requerimientos de seguridad diferentes dentro de cada uno de los dominios.

Este tipo de perímetro de red se puede implementar instalando un gateway seguro entre dos redes para mantenerlas interconectadas y controlar el acceso y el flujo de información entre los dos dominios. Este gateway debiera estar configurado para filtrar el tráfico entre estos dominios (ver 11.4.6 y 11.4.7) y para bloquear el acceso no-autorizado en concordancia con la política de control de acceso de la organización. Un ejemplo de este tipo de gateway es lo que comúnmente se conoce como un firewall. Otro método para segregar dominios lógicos separados es restringir el acceso a la red utilizando redes privadas virtuales para grupos de usuarios dentro de la organización.

Las redes también pueden ser segregadas utilizando la funcionalidad del dispositivo de red; por ejemplo, IP switching. Los dominios separados también se pueden implementar controlando los flujos de data a la red utilizando capacidades routing/switching, como listas de control de acceso.

El criterio de segregación de las redes en dominios se debiera basar en la política de control de acceso y los requerimientos de acceso (ver 10.1), y también debiera tomar en cuenta el costo relativo y el impacto en el desempeño al incorporar una adecuada tecnología de routing o gateway de red.

Además, la segregación de las redes se debiera basar en el valor y la clasificación de la información almacenada o procesada en la red, niveles de confianza o líneas comerciales; para así reducir el impacto total de una interrupción del servicio.

Se debiera tener en consideración la segregación de las redes inalámbricas de las redes internas y privadas. Como los perímetros de las redes inalámbricas no están bien definidos, se debiera llevar a cabo una evaluación del riesgo para identificar los controles (por ejemplo, autenticación sólida, métodos criptográficos y selección de frecuencia) para mantener la segregación de la red.

Otra información

Las redes se están extendiendo cada vez más allá de los límites organizacionales tradicionales, conforme se forman sociedades comerciales que puedan requerir la interconexión o intercambio de medios de procesamiento de la información y redes. Estas extensiones podrían incrementar el riesgo de un acceso no-autorizado a los sistemas de información existentes que utilizan la red, algunos de los cuales pueden requerir protección de otros usuarios de la red debido a la confidencialidad o grado crítico.

11.4.6 Control de conexión a la red

Control

Para las redes compartidas, especialmente aquellas que se extienden a través de las fronteras de la organización, se debiera restringir la capacidad de los usuarios para conectarse a la red, en línea con la política de control de acceso y los requerimientos de las aplicaciones comerciales (ver 11.1).

Lineamiento de implementación

Los derechos de acceso a la red de los usuarios se debieran mantener y actualizar conforme lo requiera la política de control de acceso (ver 11.1.1).

Se puede restringir la capacidad de conexión de los usuarios a través de gateways de la red que filtran el tráfico por medio de tablas o reglas predefinidas. Los ejemplos de aplicaciones a las cuales se pueden aplicar las restricciones son:

a) mensajes; por ejemplo, correo electrónico,
b) transferencia de archivos,
c) acceso interactivo,
d) acceso a una aplicación.

Se debieran considerar vincular los derechos de acceso a la red con ciertos días u horas.

Otra información

La política de control de acceso puede requerir la incorporación de los controles para restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites o fronteras organizacionales.

11.4.7 Control de routing de la red

Control

Se debieran implementar controles de routing en las redes para asegurar que las conexiones de la computadora y los flujos de información no violen la política de control de acceso de las aplicaciones comerciales.

Si se emplean tecnologías “proxy” (en inglés, representante o apoderado) y/o de traducción de direcciones de la red, se pueden utilizar los gateways de seguridad para validar las direcciones de la fuente y el destino en los puntos de control de las redes internas y externas. Los encargados de la implementación debieran estar al tanto de las fuerzas y debilidades de

cualquier mecanismo empleado. Los requerimientos para el control del routing de la red se debieran basar en la política de control de acceso (ver 11.1).

Otra información

Las redes compartidas, especialmente aquellas que se extienden a través de las fronteras organizacionales, pueden requerir controles de routing adicionales. Esto se aplica particularmente cuando las redes son compartidas con terceros (no-organización).

11.5 Control del acceso al sistema operativo

Objetivo: Evitar el acceso no autorizado a los sistemas operativos.

Se debieran utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios debieran tener la capacidad para:

a) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;
b) registrar los intentos exitosos y fallidos de autenticación del sistema;
c) registrar el uso de los privilegios especiales del sistema;
d) emitir alarmas cuando se violan las políticas de seguridad del sistema;
e) proporcionar los medios de autenticación apropiados;
f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

11.5.1 Procedimientos para un registro seguro

Control

El acceso a los sistemas operativos debiera ser controlado mediante un procedimiento de registro seguro.

Lineamiento de implementación

El procedimiento para registrarse en un sistema de operación debiera ser diseñado de manera que minimice la oportunidad de un acceso no autorizado. Por lo tanto, el procedimiento para registrarse debiera divulgar el mínimo de información acerca del sistema para evitar proporcionar al usuario no-autorizado ninguna ayuda innecesaria. Un buen procedimiento de registro:

a) no debiera mostrar identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro;

b) debiera mostrar la advertencia general que a la computadora sólo pueden tener acceso los usuarios autorizados;
c) no debiera proporcionar mensajes de ayuda durante el procedimiento de registro que ayuden al usuario no-autorizado;
d) sólo debiera validar la información del registro después de completar todo el input de data. Si surge una condición de error, el sistema debiera indicar qué parte de la data es correcta o incorrecta;
e) debiera limitar el número de intentos de registro infructuosos permitidos; por ejemplo, tres intentos; y debiera considerar:
    1) registrar los intentos exitosos y fallidos;
    2) forzar un tiempo de espera antes de permitir más intentos de registro o rechazar cualquier otro intento sin una autorización específica;
    3) desconectar las conexiones de vínculo a la data;
    4) establecer el número de re-intentos de clave secreta en conjunción con el largo mínimo de la clave secreta y el valor del sistema que se está protegiendo;
f) debiera limitar el tiempo máximo y mínimo permitido para el procedimiento de registro. Si se excede este tiempo, el sistema debiera terminar el registro;
g) debiera mostrar la siguiente información a la culminación de un registro satisfactorio:
    1) fecha y hora del registro satisfactorio previo;
    2) detalles de cualquier intento infructuoso desde el último registro satisfactorio;
h) no debiera mostrar la clave secreta que se está ingresando o considerar esconder los caracteres de la clave secreta mediante símbolos;
i) no debiera transmitir claves secretas en un texto abierto a través de la red.

Otra información

Si las claves secretas se transmiten a través de la red en un texto abierto durante la sesión, estas pueden ser capturadas por un programa espía en la red.

11.5.2 Identificación y autenticación del usuario

Control

Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debiera escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario.

Lineamiento de implementación

Se debiera aplicar este control a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes, programadores de sistemas y administradores de bases de datos).

Se debieran utilizar los IDs de usuarios para rastrear las actividades hasta la persona responsable. Las actividades de usuarios regulares no debieran realizarse desde cuentas privilegiadas.

En circunstancias individuales, cuando existe un beneficio comercial claro, se puede utilizar un ID de usuario compartido para un grupo de usuarios o un trabajo específico. Para tales casos la aprobación de la gerencia debiera estar documentada. Se pueden requerir controles adicionales para mantener la responsabilidad.

Sólo se debiera permitir el uso de IDs genéricos para una persona cuando las funciones accesibles o acciones llevadas a cabo por el ID no necesitan ser rastreadas (por ejemplo, sólo acceso de lectura), o cuando existen otros controles establecidos (por ejemplo, la clave secreta para un ID genérico sólo es emitido para una persona a la vez y se registra dicha instancia).

Cuando se requiere autenticación y verificación de identidad sólidas, se debieran utilizar métodos de autenticación alternativos para las claves secretas, como los medios criptográficos, tarjetas inteligentes, dispositivos o medios biométricos.

Otra información

Las claves secretas (ver también 11.3.1 y 11.5.3) son una manera muy común para proporcionar identificación y autenticación en base a un secreto que sólo conoce el usuario. Se puede lograr lo mismo con medios criptográficos y protocolos de autenticación. La fuerza de la identificación y autenticación del usuario debiera ser la adecuada para la confidencialidad de la información a la cual se va a tener acceso.

Los objetos como los dispositivos de memoria o tarjetas inteligentes que poseen los usuarios también pueden ser utilizados para la identificación y autenticación. También se pueden utilizar tecnologías de autenticación biométrica que utilizan las características o atributos singulares de una persona para autenticar su identidad. Una combinación de tecnologías y mecanismos vinculados de manera segura proporcionarán una autenticación más sólida.

11.5.3 Sistema de gestión de claves secretas

Control

Los sistemas para el manejo de claves secretas debieran ser interactivos y debieran asegurar claves secretas adecuadas.

Lineamiento de implementación

Un sistema de gestión de claves secretas:

a) aplicar el uso de IDs de usuarios individuales y claves secretas para mantener la responsabilidad;
b) permitir a los usuarios seleccionar y cambiar sus propias claves secretas e incluir un procedimiento de confirmación para permitir errores de input;
c) aplicar la elección de claves secretas adecuadas (ver 11.3.1);
d) aplicar los cambios de claves secretas (ver 11.3.1);
e) obligar a los usuarios a cambiar las claves secretas temporales en su primer ingreso o registro (ver 11.2.3);
f) mantener un registro de claves de usuario previas y evitar el re-uso;
g) no mostrar las claves secretas en la pantalla en el momento de ingresarlas;
h) almacenar los archivos de claves secretas separadamente de la data del sistema de aplicación;
i) almacenar y transmitir las claves secretas en un formato protegido (por ejemplo, codificado o indexado).

Otra información

Las claves secretas son uno de los principales medios para validar la autoridad del usuario para tener acceso a un servicio de cómputo.

Algunas aplicaciones requieren que una autoridad independiente asigne claves secretas de usuario; en tales casos, no se aplican los puntos b), d) y e) del lineamiento anterior. En la mayoría de los casos, las claves secretas son seleccionadas y mantenidas por los usuarios. Ver a sección 11.3.1 para lineamientos sobre el uso de claves secretas.

11.5.4 Uso de las utilidades del sistema

Control

Se debiera restringir y controlar estrechamente el uso de los programas de utilidad que podrían ser capaces de superar los controles del sistema y la aplicación.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para el uso de las utilidades del sistema:

a) uso de los procedimientos de identificación, autenticación y autorización para las utilidades del sistema;´

b) segregación de las utilidades del sistema del software de la aplicación;
c) limitar el uso de las utilidades del sistema a un número práctico mínimo de usuarios autorizados y confiables (ver 11.2.2);
d) autorización para el uso ad hoc de las utilidades del sistema;
e) limitación de la disponibilidad de las utilidades del sistema; por ejemplo, por la duración de un cambio autorizado;
f) registro de todo uso de las utilidades del sistema;
g) definir y documentar los niveles de autorización de las utilidades del sistema;
h) eliminación o inutilizar todas las utilidades innecesarias basadas en software, así como los software del sistema que sean innecesarios;
i) no poner las utilidades a disposición de los usuarios que tienen acceso a las aplicaciones en los sistemas donde se requiere la segregación de los debierares.

Otra información

La mayoría de las instalaciones de cómputo tienen uno o más programas de utilidades del sistema que podrían superar los controles del sistema y la aplicación.

11.5.5 Cierre de una sesión por inactividad

Control

Las sesiones inactivas debieran ser cerradas después de un período de inactividad definido.

Lineamiento de implementación

Un dispositivo de cierre debiera borrar la pantalla de la sesión y también, posiblemente más adelante, cerrar la aplicación y las sesiones en red después de un período de inactividad definido. El tiempo de espera antes del cierre debiera reflejar los riesgos de seguridad del área, la clasificación de la información que está siendo manejada y la aplicación siendo utilizada, y los riesgos relacionados con los usuarios del equipo.

Una forma limita del dispositivo de cierre puede ser provista para algunos sistemas, este dispositivo borra la pantalla y evita el acceso no autorizado pero no cierra las sesiones de la aplicación o la red.

Otra información

Este control es particularmente importante en las ubicaciones de alto riesgo, las cuales incluyen áreas públicas o externas fuera de la gestión de seguridad de la organización. Se debieran cerrar las sesiones para evitar el acceso no autorizado de personas y la negación de ataques del servicio.

11.5.6 Limitación del tiempo de conexión

Control

Se debieran utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional para las aplicaciones de alto riesgo.

Lineamiento de implementación

Se debieran considerar controles sobre el tiempo de conexión para las aplicaciones de cómputo sensibles, especialmente desde ubicaciones de alto riesgo; por ejemplo, áreas públicas o externas que están fuera de la gestión de seguridad de la organización. Los ejemplos de tales restricciones incluyen:

a) utilizar espacios de tiempo predeterminados; por ejemplo, para transmisiones de archivos en lotes, o sesiones interactivas regulares de corta duración;
b) restringir los tiempos de conexión a los horarios laborales normales, si no existe ningún requerimiento para sobre-tiempo o una operación de horario extendido;
c) considerar la re-autenticación cada cierto intervalo de tiempo.

Otra información

Limitar el período permitido para las conexiones con los servicios de cómputo reduce la ventana de oportunidad para el acceso no autorizado. Limitar la duración de las sesiones activas evita que los usuarios mantengan sesiones abiertas para evitar la re-autenticación.

11.6 Control de acceso a la aplicación y la información

Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

Se debieran utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.

El acceso lógico al software de la aplicación y la información se debiera limitar a los usuarios autorizados. Los sistemas de aplicación debieran:

a) controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida;
b) proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación;
c) no comprometer a otros sistemas con los cuales se comparten recursos de información.

11.6.1 Restricción del acceso a la información

Control

El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debiera limitarse en concordancia con la política de control de acceso definida.

Lineamiento de implementación

Las restricciones para el acceso se debieran basar en los requerimientos de las aplicaciones comerciales individuales. La política de control de acceso también debiera ser consistente con la política de acceso organizacional (ver sección 11.1).

Se debiera considerar aplicar los siguientes lineamientos para reforzar los requerimientos de restricción del acceso:

a) proporcionar menús para controlar el acceso a las funciones del sistema de aplicación;
b) controlar los derechos de acceso de los usuarios; por ejemplo, lectura, escritura, eliminar y ejecutar;
c) controlar los derechos de acceso de otras aplicaciones;
d) asegurar que los outputs de los sistemas de aplicación que manejan información confidencial sólo contengan la información relevante para el uso del output y sólo sea enviada a las terminales y ubicaciones autorizadas; esto debiera incluir revisiones periódicas de dichos outputs para asegurar que se descarte la información redundante.

11.6.2 Aislar el sistema confidencial

Control

Los sistemas confidenciales debieran tener un ambiente de cómputo dedicado (aislado).

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para aislar el sistema sensible o confidencial:

a) el propietario de la aplicación debiera identificar y documentar explícitamente la sensibilidad o confidencialidad del sistema de aplicación;
b) cuando una aplicación confidencial va a correr en un ambiente compartido, el propietario de la aplicación confidencial debiera identificar y aceptar los sistemas de aplicación con los cuales va a compartir recursos y los riesgos correspondientes.

Otra información

Algunos sistemas de aplicación son lo suficientemente sensibles a una pérdida potencial que requieren un manejo especial. Esta sensibilidad puede indicar que el sistema de aplicación:

a) debiera correr un una computadora dedicada; o

b) sólo debiera compartir recursos con sistemas de aplicaciones confiables.

El aislamiento se debiera lograr utilizando métodos físicos o lógicos (ver también 11.4.5).

11.7 Computación y tele-trabajo móvil

Objetivo: Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles. La protección requerida se debiera conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se debieran considerar los riesgos de trabajar en un ambiente desprotegido y se debiera aplicar la protección apropiada. En el caso del tele-trabajo, la organización debiera aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

11.7.1 Computación y comunicaciones móviles

Control

Se debiera establecer una política y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móvil.

Lineamiento de implementación

Cuando se utiliza medios de computación y comunicación móvil; por ejemplo, notebooks, palmtops, laptops, tarjetas inteligentes y teléfonos móviles; se debiera tener especial cuidado en asegurar que no se comprometa la información comercial. La política de computación móvil debiera tomar en cuenta los riesgos de trabajar con equipo de computación móvil en ambientes desprotegidos.

La política de computación móvil debiera incluir los requerimientos de protección física, controles de acceso, técnicas criptográficas, respaldos (back-up) y protección contra virus. Esta política también debiera incluir reglas y consejos para la conexión de medios móviles con las redes y lineamientos para el uso de estos medios en lugares públicos.

Se debiera tener cuidado cuando se utiliza medios de computación móvil en lugares públicos, salas de reuniones y otras áreas desprotegidas fuera de los locales de la organización. Se debiera establecer la protección para evitar el acceso no autorizado o divulgación de la información almacenada y procesada por estos medios; por ejemplo, utilizando técnicas criptográficas (ver 12.3).

Los usuarios de los medios de computación móvil que se encuentran en lugares públicos debieran tener cuidado en evitar que personas no autorizadas vean su trabajo. Se debiera establecer procedimientos contra los software maliciosos y se debieran mantener actualizados (ver 10.4).

Los respaldos (back-up) de la información comercial crítica se debieran realizar con regularidad. Debiera estar disponible el equipo para permitir realizar un respaldo rápido y fácil de la información. Se debiera dar a estos respaldos la protección adecuada; por ejemplo, contra el robo o pérdida de información.

Se debiera dar la protección adecuada al uso de medios móviles conectados a las redes. El acceso remoto a la información comercial a través de una red pública utilizando medios de computación móvil sólo debiera realizarse después de una satisfactoria identificación y autenticación, y con los controles de acceso adecuados en funcionamiento.

Los medios de computación móvil también debieran estar físicamente protegidos contra robo especialmente cuando se les deja en, por ejemplo, autos y otros medios de transporte, cuartos de hotel, centros de conferencias y lugares de reunión. Se debiera establecer un procedimiento específico tomando en cuenta los requerimientos legales, de seguros y otros requerimientos de seguridad de la organización para casos de robo o pérdida de los medios móviles. El equipo que contiene información comercial importante, confidencial y/o crítica no se debiera dejar desatendido y, cuando sea posible, debiera estar asegurado físicamente, o se pueden utilizar seguros para proteger el equipo (ver 9.2.5).

Se debiera planear capacitación para el personal que utiliza computación móvil para elevar el nivel de conciencia sobre los riesgos adicionales resultantes de esta forma de trabajo y los controles que se debieran implementar.

Otra información

Las conexiones inalámbricas a la red móvil son similares a otros tipos de conexión en red, pero tienen diferencias importantes que se debieran considerar cuando se identifican los controles. Las diferencias típicas son

a) algunos protocolos de seguridad inalámbricos aún son inmaduros y tienen debilidades conocidas;
b) la información almacenada en las computadoras móviles tal vez no tiene respaldo (back-up) debido a la banda ancha limitada de la red y/o porque el equipo móvil puede no estar conectado en las horas en que se realizan los respaldos.

11.7.2 Tele-trabajo

Control

Se debiera desarrollar e implementar una política, planes operacionales y procedimientos para las actividades de tele-trabajo.

Lineamiento de implementación

Las organizaciones sólo debieran autorizar las actividades de tele-trabajo si están seguros que se cuenta con los arreglos y controles de seguridad apropiados, y que estos cumplen con la política de seguridad de la organización.

El lugar del tele-trabajo debiera contar con una protección adecuada contra; por ejemplo, el robo de equipo e información, la divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el mal uso de los medios. Las actividades de tele-trabajo debieran ser autorizadas y controladas por la gerencia, y se debiera asegurar que se hayan establecido los arreglos adecuados para esta forma de trabajo.

Se debieran considerar los siguientes puntos:

a) la seguridad física existente en el lugar del tele-trabajo, tomando en cuenta la seguridad física del edificio y el ambiente del local:
b) el ambiente de tele-trabajo físico propuesto;
c) los requerimientos de seguridad de las comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la confidencialidad de la información a la cual se tendrá acceso y el vínculo de comunicación y confidencialidad del sistema interno;
d) la amenaza de acceso no autorizado a la información o recursos por parte de otras personas que utilizan el medio; por ejemplo, familia y amigos;
e) el uso de redes en casa y los requerimientos o restricciones en la configuración de los servicios de la red inalámbrica;
f) las políticas y procedimientos para evitar las disputas relacionadas con los derechos de propiedad intelectual desarrollados en equipo de propiedad privada;
g) acceso a equipo de propiedad privada (para chequear la seguridad de la máquina o durante una investigación), el cual puede ser evitado por la legislación;

h) contratos de licencias de software que hacen que las organizaciones sean responsables por las licencias del software del cliente en las estaciones de trabajo de propiedad de los empleados, contratistas y terceros;
i) requerimientos de protección anti-virus y firewall.

Los lineamientos y arreglos a considerarse debieran incluir:

a) la provisión de equipo y muebles de almacenaje adecuados para las actividades de tele-trabajo, donde no está permitido el uso del equipo de propiedad privada que no esté bajo el control de la organización;
b) una definición del trabajo permitido, el horario de trabajo, la clasificación de la información que se puede mantener y los sistemas y servicios internos a los cuales tiene autorización de acceso la persona que realiza el tele-trabajo;
c) la provisión de un equipo de comunicación adecuado, incluyendo métodos para asegurar el acceso remoto;
d) seguridad física;
e) reglas y lineamientos sobre el acceso de la familia y amigos al equipo y la información;
f) la provisión de soporte y mantenimiento de hardware y software;
g) la provisión de un seguro;
h) los procedimientos para el respaldo (back-up) y la continuidad del negocio;
i) monitoreo de la auditoría y la seguridad;
j) revocación de los derechos de autoridad y acceso, y la devolución del equipo cuando terminan las actividades de tele-trabajo.

Otra información

El tele-trabajo utiliza tecnología de comunicaciones que permite al personal trabajar remotamente desde un lugar fijo fuera de su organización.

12 Adquisición, desarrollo y mantenimiento de los sistemas de información

12.1 Requerimientos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad sea una parte integral de los sistemas de información. Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones comerciales, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso comercial puede ser crucial para la seguridad. Se debieran identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

Se debieran identificar todos los requerimientos de seguridad en la fase de requerimientos de un proyecto; y debieran ser justificados, acordados y documentados como parte del caso comercial general para un sistema de información.

12.1.1 Análisis y especificación de los requerimientos de seguridad

Control

Los enunciados de los requerimientos comerciales para los sistemas de información nuevos, o las mejoras a los sistemas de información existentes, debieran especificar los requerimientos de los controles de seguridad.

Los requerimientos y los controles de seguridad debieran reflejar el valor comercial de los activos de información involucrados (ver también 7.2), y el daño comercial potencia que podría resultar de una falla o ausencia de seguridad.

Los requerimientos de seguridad para a seguridad de la información y los procesos para implementar la seguridad debieran ser integrados en las primeras etapas de los proyectos de sistemas de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si los productos son comprados, se debiera realizar un proceso de prueba y adquisición formal. Los contratos con el proveedor debieran tratar los requerimientos de seguridad identificados. Cuando la funcionalidad de seguridad de un producto propuesto no satisface el requerimiento especificado entonces se debieran reconsiderar el riesgo introducido y los controles asociados antes de comprar el producto. Donde se suministra funcionalidad adicional y causa un riesgo de seguridad, este debiera ser desactivado o se debiera revisar la estructura de control propuesta para determinar si se puede obtener alguna ventaja de la funcionalidad mejorada disponible.

Otra información

Si se considera apropiado, por ejemplo por razones de costo, la gerencia puede desear hacer uso de productos evaluados y certificados independientemente. Se puede encontrar mayor información sobre el criterio de evaluación de los productos de seguridad TI en ISO/IEC 15408 u otros estándares de certificación o evaluación, conforme sea apropiado.

ISO/IEC TR 13335-3 proporciona un lineamiento sobre el uso de procesos de gestión de riesgo para identificar los requerimientos para los controles de seguridad.

12.2 Procesamiento correcto en las aplicaciones

Objetivo: Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones. Se debieran diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para asegurar un procesamiento correcto. Estos controles debieran incluir la validación de la input data, procesamiento interno y output data. Se pueden requerir controles adicionales para los sistemas que procesan, o tienen impacto sobre, la información confidencial, valiosa o crítica. Estos controles se debieran determinar sobre la base de los requerimientos de seguridad y la evaluación del riesgo.

12.2.1 Validación de la input data

Control

Se debiera validar la input data para las aplicaciones para asegurar que esta data sea correcta y apropiada.

Lineamiento de implementación

Se debieran realizar chequeos del input de las transacciones comerciales, la data fija (por ejemplo nombres y direcciones, límites de crédito, números de referencia de los clientes), y tablas de parámetros (por ejemplo; precios de venta, moneda, tasas de cambio, tasa tributaria). Se debieran considerar los siguientes lineamientos:

a) input dual u otros chequeos de data; tales como chequeo de límites o limitar los campos a los rangos específicos de la input data; para detectar los siguientes errores:
    1) valores fuera de rango;
    2) caracteres inválidos en los campos de data;
    3) data incompleta o faltante;
    4) exceder los límites superiores e inferiores del volumen de data;
    5) data de control no autorizada o inconsistente;
b) revisión periódica del contenido de los campos claves o archivos de data para confirmar su validez e integridad;
c) inspeccionar los documentos de input de la copia impresa en caso de cambios no autorizados (todos los cambios a los documentos de input debieran ser autorizados);

d) procedimientos para responder a los errores de validación;
e) procedimientos para probar la plausibilidad de la input data;
f) definir las responsabilidades de todo el personal involucrado en el proceso de input de data;
g) crear un registro de las actividades involucradas en el proceso de input de data (ver 10.10.1).

Otra información

Cuando sea aplicable, se debiera considerar el examen y validación automática de la input data para reducir el riesgo de errores y evitar los ataques estándar incluyendo el desbordamiento de la memoria intermedia y la inyección de un código.

12.2.2 Control del procesamiento interno

Control

Los chequeos de validación se debieran incorporar en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

Lineamiento de implementación

El diseño e implementación de las aplicaciones debiera asegurar que se minimicen los riesgos de fallas en el procesamiento que lleven a la pérdida de la integridad. Las áreas específicas a considerarse incluyen:

a) el uso de funciones agregadas, modificadas y eliminadas para implementar cambios en la data;
b) los procedimientos para evitar que los programas corran en el orden equivocado o corran después de una falla en el procesamiento previo (ver también 10.1.1);
c) el uso de programas apropiados para recuperarse de fallas para asegurar el correcto procesamiento de la data;
d) protección contra ataques utilizando excesos/desbordamientos de la memora intermedia.

Se debiera preparar una lista de chequeo apropiada, se debieran documentar las actividades y los resultados se debieran mantener seguros. Los ejemplos de los chequeos que se pueden incorporar incluyen lo siguiente:

a) controles de sesión o lote, para conciliar los saldos del archivo de data después de las actualizaciones de la transacción;
b) controles de saldos, para chequear los saldos de apertura comparándolos con los saldos de cierre anteriores; específicamente:
    1) controles corrida-a-corrida;

2) totales de actualización del archivo;
3) controles programa-a-programa;

c) validación de la input data generada por el sistema (ver 12.2.1);
d) chequeos de la integridad, autenticidad y cualquier otro dispositivo de seguridad de la data o software cargado o descargado, entre la computadora central y las remotas;
e) totales hash de registros y archivos;
f) chequeos para asegurar que los programas se corran en el momento adecuado;
g) chequeos para asegurar que los programas sean corridos en el orden correcto y terminados en caso de una falla, y que se detenga el procesamiento hasta que se resuelva el problema;
h) crear un registro de las actividades involucradas en el procesamiento (ver 10.10.1).

Otra información

La data que ha sido correctamente ingresada puede verse corrompida por errores en el hardware, errores en el procesamiento o a través de actos deliberados. Los chequeos de validación requeridos dependerán de la naturaleza de la aplicación y el impacto comercial de cualquier corrupción de la data.

12.2.3 Integridad del mensaje

Control

Se debiera identificar los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, y se debieran identificar e implementar los controles apropiados.

Lineamiento de implementación

Se debiera realizar una evaluación de los riesgos de seguridad para determinar si se requiera la integridad del mensaje y para identificar el método de implementación más apropiado.

Otra información

Se pueden utilizar técnicas criptográficas (ver 12.3) como un medio apropiado para implementar la autenticación del mensaje.

12.2.4 Validación de la output data

Control

Se debiera validar la output data de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y el apropiado para las circunstancias.

Lineamiento de implementación

La validación del output puede incluir:

a) chequeos de plausibilidad para comprobar si el output data es razonable;
b) conteo de control de conciliación para asegurar el procesamiento de toda la data;
c) proporcionar la información suficiente para un lector o el sistema de procesamiento subsiguiente para determinar la exactitud, integridad, precisión y clasificación de la información;
d) procedimientos para responder a las pruebas de validación de output;
e) definir las responsabilidades de todo el personal involucrado en el proceso de output de data;
f) crear un registro de las actividades en el proceso de validación del output de data.

Otra información

Típicamente, los sistemas y aplicaciones son elaborados sobre la premisa que si han pasado por la apropiada validación, verificación y prueba; el output siempre será el correcto. Sin embargo, esta premisa no es siempre válida; es decir, aún los sistemas que han sido probados pueden producir output incorrecto en algunas circunstancias.

12.3 Controles criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos. Se debiera desarrollar una política sobre el uso de controles criptográficos. Se debiera establecer una gestión clave para sostener el uso de técnicas criptográficas.

12.3.1 Política sobre el uso de controles criptográficos

Control

Se debiera desarrollar e implementar una política sobre el uso de controles criptográficos para proteger la información.

Lineamiento de implementación

Cuando se desarrolla una política criptográfica se debiera considerar lo siguiente:

a) el enfoque gerencial sobre el uso de los controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales se debiera proteger la información comercial (ver también 5.1.1);

b) en base a la evaluación del riesgo, se debiera identificar el nivel de protección requerido tomando en cuenta el tipo, fuerza y calidad del algoritmo criptográfico requerido;

c) el uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles o removibles o a través de las líneas de comunicación;

d) el enfoque de la gestión de claves, incluyendo los métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves pérdidas, comprometidas o dañadas;

e) roles y responsabilidades; por ejemplo, quién es responsable de:
   1) la implementación de la política;
   2) la gestión de claves, incluyendo la generación de claves (ver también 12.3.2);

f) los estándares a adoptarse para la implementación efectiva en toda la organización (cuál solución se utiliza para cuáles procesos comerciales);

g) el impacto de utilizar información codificada sobre los controles que se basan en la inspección del contenido(por ejemplo, detección de virus);

Cuando se implementa la política criptográfica de la organización, se debiera considerar las regulaciones y las restricciones nacionales que se podrían aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los problemas del flujo inter-fronteras de la información codificada (ver también 15.1.6).

Se pueden utilizar controles criptográficos para lograr diferentes objetivos de seguridad:

a) confidencialidad: utilizando la codificación de la información para proteger la información confidencial o crítica, ya sea almacenada o transmitida;

b) integridad/autenticidad: utilizando firmas digitales o códigos de autenticación del mensaje para proteger la autenticidad e integridad de la información confidencial o crítica almacenada o transmitida;

c) no-repudiación: utilizando técnicas criptográficas para obtener prueba de a ocurrencia o no-ocurrencia de un evento o acción.

Otra información

La decisión de si es apropiada una solución criptográfica debiera ser vista como parte de un proceso más amplio de evaluación del riesgo y selección de controles. Luego esta evaluación

se puede utilizar para determinar si es apropiado un control criptográfico, qué tipo de control se debiera aplicar, y para cuáles propósitos y procesos comerciales.

Es necesaria una política sobre el uso de controles criptográficos para maximizar los beneficios y minimizar los riesgos de utilizar técnicas criptográficas, y evitar el uso inapropiado o incorrecto. Cuando se utilizan firmas digitales, se debiera considerar cualquier legislación relevante, en particular la legislación que describe las condiciones bajo las cuales una firma digital es aceptada legalmente (ver 15.1).

Se debiera buscar asesoría especialista para identificar el nivel de protección apropiado y definir las especificaciones adecuadas que proporcionarán la protección y el soporte requeridos para la implementación de un sistema de gestión de claves a seguir (ver también 12.3.2).

ISO/IEC JTC1 SC27 ha desarrollado varios estándares relacionados con los controles criptográficos. Se puede encontrar mayor información en IEEE P1363 y los Lineamientos sobre Criptografía OEECD.

12.3.2 Gestión de claves

Control

Se debiera establecer la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

Lineamiento de implementación

Todas las claves criptográficas debieran estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación no-autorizada. Se debiera proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.

El sistema de gestión de claves se debiera basar en un conjunto de estándares, procedimientos y métodos seguros acordados para:

a) generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones;
b) generar y obtener certificados de claves públicas;
c) distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas;
d) almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves;

e) cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debieran cambiar las claves y cómo se realiza esto;

f) lidiar con las claves comprometidas;

g) revocar las claves incluyendo cómo se debieran retirar o desactivar las claves; por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la organización (en cuyos casos las claves también debieran ser archivadas);

h) recuperar las claves cuando han sido perdidas o corrompidas como parte de la continuidad y gestión del negocio; por ejemplo, para recuperar la información codificada;

i) archivar las claves; por ejemplo, para la información archivada o respaldada;

j) destruir las claves;

k) registrar y auditar las actividades relacionadas con la gestión de claves.

Para poder reducir la posibilidad de comprometer las claves, se debieran definir las fechas de activación y desactivación para que las claves sólo se puedan utilizar durante un período de tiempo limitado. El período de tiempo dependerá de las circunstancias bajo las cuales se está utilizando el control criptográfico, y el riesgo percibido.

Además del manejo seguro de las claves secretas y privadas, también se debiera considerar la autenticidad de las claves públicas. Este proceso de autenticación se puede realizar utilizando certificados de claves públicas, los cuales normalmente son emitidos por una autoridad de certificación, la cual debiera ser una organización reconocida con controles y procedimientos adecuados para proporcionar el grado de confianza requerido.

Los contenidos de los acuerdos o contratos de nivel de servicio con los proveedores externos de servicios de criptografía; por ejemplo, una autoridad de certificación; debieran abarcar los temas de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la provisión de los servicios (ver 6.2.3).

Otra información

La gestión de las claves criptográficas es esencial para el uso efectivo de las técnicas criptográficas. ISO/IEC 11770 proporciona mayor información sobre la gestión de las claves. 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 utilizada tanto para codificar como descodificar la información, esta clave debiera mantenerse en secreto ya que cualquiera que tenga acceso a la clave

puede decodificar toda la información codificada con esa clave o puede introducir información no-autorizada utilizando la clave:

b) técnicas de claves públicas, donde cada usuario tiene un par de claves, una clave pública (que puede ser revelada a cualquiera) y una clave privada (que se tiene que mantener en secreto); se pueden utilizar las técnicas de claves públicas para la codificación y para producir firmas digitales (ver también ISO/IEC 9796 y ISO/IEC 14888).

Existe la amenaza de la falsificación de la firma digital, reemplazándola con la clave pública de un usuario. El problema es tratado mediante el uso de un certificado de clave pública.

Las técnicas criptográficas también se pueden utilizar para proteger las claves criptográficas. Tal vez se necesite considerar procedimientos para el manejo legal del acceso a las claves criptográficas; por ejemplo, tal vez se necesite la información codificada esté disponible en una forma descodificada como evidencia en un caso en la corte.

12.4 Seguridad de los archivos del sistema

Objetivo: Garantizar la seguridad de los archivos del sistema. Se debiera controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI y las actividades de soporte se debieran realizar de una manera segura.

12.4.1 Control del software operacional

Control

Se debieran establecer procedimientos para el control de la instalación del software en los sistemas operacionales.

Lineamiento de implementación

Para minimizar el riesgo de corrupción de los sistemas operacionales, se debieran considerar los siguientes lineamientos para controlar los cambios:

a) la actualización del software operacional, aplicaciones y bibliotecas de programas sólo debiera ser realizada por administradores capacitados con la apropiada autorización gerencial (ver 12.4.3);

b) los sistemas operacionales sólo debieran mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

c) el software de las aplicaciones y el sistema de operación sólo se debiera implementar después de una prueba extensa y satisfactoria; las pruebas debieran incluir pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se debieran llevar a cabo en sistemas separados (ver también 10.1.4); se debiera asegurar que se hayan actualizado todas las bibliotecas fuente correspondientes del programa;

d) se debiera utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema;

e) se debiera establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios;

f) se debiera mantener un registro de auditoría de todas las actualizaciones a las bibliotecas del programa operacional;

g) se debieran mantener las versiones previas del software de aplicación como una medida de contingencia;

h) se debieran archivar las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo.

El software provisto por un vendedor y utilizado en el sistema operacional se debiera mantener en el nivel donde recibe soporte del proveedor. A lo largo del tiempo, los proveedores dejarán de dar soporte a las versiones más antiguas del software. La organización debiera considerar los riesgos de trabajar con software que no cuenta con soporte.

Cualquier decisión para actualizar a una versión nueva debiera tomar en cuenta los requerimientos comerciales para el cambio, y la seguridad de la versión; es decir, la introducción de la nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión. Se pueden aplicar algunos parches de software cuando ayudan a remover o reducir las debilidades de seguridad (ver también 12.6.1).

Sólo se debiera dar a los proveedores acceso físico o lógico para propósitos de soporte cuando sea necesario, y con aprobación de la gerencia. Se debieran monitorear las actividades del proveedor

El software de cómputo puede constar del software y módulos suministrados externamente, el cual se debiera monitorear y controlar para evitar los cambios no-autorizados, los cuales introducen debilidades en la seguridad.

Otra información

Los sistemas de operación sólo se debieran actualizar cuando existe el requerimiento para hacerlo, por ejemplo, si la versión actual del sistema de operación ya no soporta los requerimientos comerciales. Las actualizaciones no se realizan simplemente porque esté disponible una versión nueva del sistema de operación. Las versiones nuevas del sistema de operación pueden ser menos seguras, menos estables y menos entendibles que la versión actual.

12.4.2 Protección de la data del sistema

Control

La data de prueba se debiera seleccionar cuidadosamente, y se debiera proteger y controlar.

Lineamiento de implementación

Se debiera evitar el uso de bases de datos operacionales conteniendo información personal o cualquier otra información confidencial para propósitos de pruebas. Si la información personal o de otra manera confidencial se utiliza para propósitos de prueba, todos los detalles confidenciales debieran ser removidos o modificados más allá de todo reconocimiento antes de utilizarlos. Cuando se utiliza la data operacional para propósitos de prueba se debieran aplicar los siguientes lineamientos para protegerla:

a) procedimientos de control de acceso, los cuales se aplican a los sistemas de aplicación operacional, y también se debieran aplicar a los sistemas de aplicación de prueba;
b) debiera existir una autorización separada para cada vez que se copia información operacional en un sistema de aplicación de prueba;
c) la información operacional debiera ser borrada de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba;
d) se debiera registrar el copiado y uso de la información operacional para proporcionar un rastro de auditoria.

Otra información

La prueba del sistema y aceptación usualmente requiere de volúmenes sustanciales de data de prueba que sea lo más cercana posible a la data operacional.

12.4 3 Control de acceso al código fuente del programa

Control

Se debiera restringir el acceso al código fuente del programa.

Lineamiento de implementación

El acceso al código fuente del programa y los ítems asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debieran controlar estrictamente para evitar la introducción de una funcionalidad no-autorizada y para evitar cambios no-intencionados. Para el código fuente del programa, esto se puede lograr controlando el almacenaje central de dicho código, preferiblemente en las bibliotecas de fuentes del programa. Se debieran considerar los siguientes lineamientos (ver también 11) para controlar el acceso a dichas bibliotecas de las fuentes del programa para reducir el potencial de corrupción de los programas de cómputo:

a) cuando sea posible, no se debieran mantener las bibliotecas de fuentes del programa en los sistemas operacionales;
b) el código fuente del programa y las bibliotecas de fuentes del programa debieran ser manejadas de acuerdo con los procedimientos establecidos;
c) el personal de soporte no debiera tener acceso irrestricto a las bibliotecas de fuentes del programa;
d) la actualización de las bibliotecas de fuentes del programa y los ítems asociados, y la emisión de las fuentes del programa para los programadores sólo se debieran realizar después de haber recibido la apropiada autorización;
e) los listados del programa se debieran mantener en un ambiente seguro (ver 10.7.4);
f) se debiera mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa;
g) el mantenimiento y copiado de las bibliotecas fuentes del programa debiera estar sujeto a procedimientos estrictos de control de cambios (ver 12.5.1).

Otra información

El código fuente del programa es un código escrito por programadores, el cual es compilado (y vinculado) para crear ejecutables. Ciertos lenguajes de programación no distinguen formalmente entre el código fuente y los ejecutables ya que los ejecutables son creados en el momento que son activados.

Los estándares ISO 10007 e ISO/IEC 12207 proporcionan mayor información sobre la 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 y la información del sistema de aplicación.

Se debiera controlar estrictamente los ambientes del proyecto y soporte.

Los gerentes responsables por los sistemas de aplicación también debieran ser responsables por la seguridad del ambiente del proyecto o el soporte. Ellos debieran asegurar que todos los cambios propuestos para el sistema sean revisados para chequear que no comprometan la seguridad del sistema o el ambiente de operación.

12.5.1 Procedimientos del control del cambio

Control

Se debiera controlar la implementación de los cambios mediante el uso de procedimientos formales para el control del cambio.

Lineamiento de la implementación

Se debieran documentar y hacer cumplir los procedimientos formales de control del cambio para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y los cambios importantes a los sistemas existentes debieran realizarse después de un proceso formal de documentación, especificación, prueba, control de calidad e implementación manejada.

Este proceso debiera incluir una evaluación del riesgo, análisis de los impactos del cambio y la especificación de los controles de seguridad necesarios. Este proceso también debiera asegurar que los procedimientos de seguridad y control existentes no se vean comprometidos, que a los programadores de soporte sólo se les proporcione acceso a aquellas partes del sistema necesarias para su trabajo, y que se obtenga el acuerdo y la aprobación formal de cualquier cambio.

Cuando sea practicable, se debieran integrar los procedimientos de control de cambio operacional y en la aplicación (ver también 10.1.2). Los procedimientos de cambio debieran incluir:

a) mantener un registro de los niveles de autorización acordados;
b) asegurar que los cambios sean presentados por los usuarios autorizados;
c) revisar los procedimientos de control e integridad para asegurar que no se vean comprometidos por los cambios;
d) identificar todo el software, información, entidades de base de datos y hardware que requieran enmiendas;
e) obtener la aprobación formal para propuestas detalladas antes de comenzar el trabajo;

f) asegurar que los usuarios autorizados acepten a los cambios antes de la implementación;
g) asegurar que el conjunto de documentación del sistema esté actualizado al completar cada cambio y que la documentación antigua se archive o se elimine;
h) mantener un control de la versión para todas las actualizaciones del software;
i) mantener un rastro de auditoría para todas las solicitudes de cambio;
j) asegurar que la documentación de operación (ver 10.1.1) y procedimientos de usuarios sean cambiados conforme sean necesarios para seguir siendo apropiados;
k) asegurar que la implementación de los cambios se realicen en el momento adecuado y no disturbe los procesos comerciales involucrados.

Otra información

El cambio de software puede tener impacto en el ambiente operacional.

La buena práctica incluye la prueba del software nuevo en un ambiente segregado de los ambientes de producción y desarrollo (ver también 10.1.4). Esto proporciona un medio para tener control sobre el software nuevo y permitir una protección adicional de la información operacional que se utiliza para propósitos de pruebas. Esto incluye parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automatizadas no se debieran utilizar en los sistemas críticos ya que algunas actualizaciones pueden causar que fallen las aplicaciones críticas (ver 12.6)

12.5.2 Revisión técnica de la aplicación después de cambios en el sistema

Control

Cuando se cambian los sistemas de operación, se debieran revisar y probar las aplicaciones comerciales críticas para asegurar que no exista un impacto adverso sobre las operaciones organizacionales o en la seguridad.

Lineamiento de implementación

Este proceso debiera abarcar:

a) revisar los procedimientos de control e integridad de la aplicación para asegurar que no se hayan visto comprometidos por los cambios en el sistema de operación:
b) asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación;
c) asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación;

d) asegurar que se realicen los cambios apropiados en los planes de continuidad del negocio (ver la cláusula 14).

Se le debiera asignar a un grupo o persona específica la responsabilidad de monitorear las vulnerabilidades y los parches y arreglos que lancen los vendedores (ver 12.6).

12.5.3 Restricciones sobre los cambios en los paquetes de software

Control

No se debieran fomentar modificaciones a los paquetes de software, se debieran limitar a los cambios necesarios y todos los cambios debieran ser estrictamente controlados.

Lineamiento de implementación

Mientras sea posible y practicable, se debieran utilizar los paquetes de software suministrados por vendedores sin modificaciones. Cuando se necesita modificar un paquete de software se debieran considerar los siguientes puntos:

a) el riesgo de comprometer los controles incorporados y los procesos de integridad;
b) si se debiera obtener el consentimiento del vendedor;
c) la posibilidad de obtener del vendedor los cambios requeridos como actualizaciones del programa estándar;
d) el impacto de si como resultado de los cambios, la organización se hace responsable del mantenimiento futuro del software.

Si son necesarios cambios, se debiera mantener el software original y se debieran aplicar los cambios en una copia claramente identificada. Se debiera implementar un proceso de gestión de actualizaciones del software para asegurar que la mayoría de los parches aprobados hasta-la-fecha y las actualizaciones de la aplicación se instalen para todo software autorizado (ver 12.6). Todos los cambios debieran ser completamente probados y documentados, de manera que puedan ser reaplicados, si fuese necesario, a las futuras actualizaciones del software. Si fuese requerido, las modificaciones debieran probadas y validadas por un organismo de evaluación independiente.

12.5.4 Filtración de información

Control

Se debieran evitar las oportunidades para la filtración de información.

Lineamiento de implementación

Se debieran considerar los siguientes puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos (covert channels):

a) escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida;
b) enmascarar y modular la conducta del sistema y las comunicaciones para reducir la probabilidad de que una tercera persona pueda deducir la información a partir de dicha conducta;
c) hacer uso de los sistemas y el software considerados de la más alta integridad; por ejemplo, utilizando productos evaluados (ver ISO/IEC 15408);
d) monitoreo regular de las actividades del personal y del sistema, cuando sea permitido bajo la legislación o regulación existente;
e) monitorear la utilización del recurso en los sistemas de cómputo.

Otra información

Los Canales Encubiertos son caminos que no están destinadas a transportar flujos de información, pero que de cualquier manera pueden existir en un sistema o red. Por ejemplo, en el manipuleo de bits se pueden utilizar paquetes de protocolo de las comunicaciones como un método escondido de señalización. Por su naturaleza, es muy difícil, sino imposible, evitar la existencia de todos los canales encubiertos posibles. Sin embargo, la explotación de dichos canales casi siempre las realiza un código Troyano (ver también 10.4.1). Por lo tanto, tomar medidas para protegerse contra códigos Troyanos reduce el riesgo de la explotación de los canales encubiertos.

El evitar el acceso no-autorizado a la red (11.4), así como las políticas y procedimientos para no fomentar el mal uso de los servicios de información por parte del personal (15.1.5), ayudarán a protegerse de los canales encubiertos.

12.5.5 Desarrollo de software abastecido externamente

Control

El desarrollo del software abastecido externamente debiera ser supervisado y monitoreado por la organización.

Lineamiento de implementación

Cuando el software es abastecido externamente, se debieran considerar los siguientes puntos:

a) contratos de licencias, propiedad de códigos, derechos de propiedad intelectual (ver 15.1.2);

b) certificación de la calidad y exactitud del trabajo llevado a cabo;
c) contratos de depósito en custodia en el evento de la falla de una tercera persona;
d) derechos de acceso para a auditoría de la calidad y seguridad del trabajo realizado;
e) requerimientos contractuales para la funcionalidad de calidad y seguridad del código;
f) prueba antes de la instalación para detectar códigos maliciosos y Troyanos.

12.6 Gestión de la Vulnerabilidad Técnica

Objetivo: Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas. Se debiera implementar una gestión de la vulnerabilidad técnica de una manera efectiva, sistemática y respetable, tomando mediciones para confirmar su efectividad. Estas consideraciones debieran incluir a los sistemas de operación, y cualquier otra aplicación en uso.

12.6.1 Control de las vulnerabilidades técnicas

Control

Se debiera obtener oportunamente la información sobre las vulnerabilidades técnicas de los sistemas de información que se están utilizando, la exposición de la organización a dichas vulnerabilidades evaluadas, y las medidas apropiadas tomadas para tratar los riesgos asociados.

Lineamiento de implementación

Un inventario actual y completo de los activos (ver 7.1) es un prerrequisito para la gestión efectiva de la vulnerabilidad técnica. La información específica necesaria para apoyar la gestión de la vulnerabilidad técnica incluye al vendedor del software, números de la versión, estado actual del empleo (por ejemplo, cuál software está instalado en cuál sistema), y la(s) persona(s) dentro de la organización responsable(s) del software.

Se debiera tomar la acción apropiada y oportuna en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se debiera seguir el siguiente lineamiento para establecer un proceso de gestión efectivo para las vulnerabilidades técnicas:

a) la organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida;

b) se debieran identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 7.1.1); estos recursos de información debieran actualizarse en base a los cambios en el inventario, o cuando se encuentran recursos nuevo o útiles;

c) se debiera definir una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes;

d) una vez que se identifica la vulnerabilidad técnica potencial, la organización debiera identificar los riesgos asociados y las acciones a tomarse; dicha acción podría involucrar el parchado de los sistemas vulnerables y/o la aplicación de otros controles;

e) dependiendo de la urgencia con que se necesita tratar la vulnerabilidad técnica, la acción a tomarse debiera realizarse de acuerdo a los controles relacionados con la gestión de cambios (ver 12.5.1) o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información (ver 13.2);

f) si es posible el parche, se debieran evaluar los riesgos asociados con instalar el parche (los riesgos impuestos por la vulnerabilidad se debieran comparar con el riesgo de instalar el parche);

g) los parches de debieran probar y evaluar antes de instalarlos para asegurar que sean efectivos y no resulten efectos secundarios que no se puedan tolerar; si el parche no está disponible, se pueden considerar otros controles:

   1) desconectar los servicios o capacidades relacionadas con la vulnerabilidad;
   2) adaptar o agregar controles de acceso; por ejemplo, firewalls en los límites de la red;
   3) mayor monitoreo para detectar o evitar ataques reales;
   4) elevar la conciencia acerca de la vulnerabilidad;
   5) mantener un registro de auditoría de todos los procedimientos realizados;
   6) el proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia;
   7) se debieran tratar primero los sistemas en alto riesgo.

Otra información

El correcto funcionamiento del proceso de gestión de la vulnerabilidad técnica de la organización es crítico para muchas organizaciones y por lo tanto, debiera ser monitoreado regularmente. Un inventario exacto es esencial para asegurar que se identifiquen las vulnerabilidades técnicas potencialmente relevantes.

La gestión de la vulnerabilidad técnica puede ser vista como una sub-función de la gestión de cambios y como tal pueden beneficiarse de los procesos y procedimientos de la gestión del cambio (ver 10.1.2 y 12.5.1).

Con frecuencia los vendedores se ven presionados a lanzar parches lo más pronto posible. Por lo tanto, un parche puede no tratar adecuadamente el problema y puede tener efectos secundarios negativos. También, en algunos casos, no es fácil desinstalar un parche una vez que este ha sido aplicado.

Si no es posible una prueba adecuada del parche; por ejemplo, debido a los costos o falta de recursos; se puede considerar una demora en el parchado para evaluar los riesgos asociados, basados en la experiencia reportada por otros usuarios.

13 Gestión de un incidente en la seguridad de la información

13.1 Reporte de los eventos y debilidades de la seguridad de la información

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna. Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales. Se les debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado.

13.1.1 Reporte de eventos en la seguridad de la información

Control

Los eventos de seguridad de la información debieran ser reportados a través de los canales gerenciales apropiados lo más rápidamente posible.

Lineamiento de implementación

Se debiera establecer un procedimiento formal para el reporte de eventos en la seguridad de la información, junto con un procedimiento de respuesta y de intensificación de incidentes,

estableciendo la acción a tomarse al recibir un reporte de un evento en la seguridad de la información. Se debiera establecer un punto de contacto para el reporte de eventos en la seguridad de la información Se debiera asegurar que este punto de contacto sea conocido a través de toda la organización, que siempre esté disponible y sea capaz de proporcionar una respuesta adecuada y oportuna.

Todos los usuarios empleados, contratistas y terceros debieran estar al tanto de la responsabilidad de reportar cualquier evento en la seguridad de la información lo más rápidamente posible. También debieran estar al tanto del procedimiento para reportar eventos en la seguridad de la información y el punto de contacto. Los procedimientos de reporte debieran incluir:

a) procesos de retroalimentación adecuados para asegurar que aquellos que reportan eventos en la seguridad de la información sean notificados de los resultados después de haber tratado y terminado con el problema;
b) formatos de reporte los eventos en la seguridad de la información para respaldar la acción de reporte, y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento en la seguridad de la información;
c) se debiera tomar la conducta correcta en el caso de un evento en la seguridad de la información; es decir
    1) anotar todos los detalles importantes inmediatamente (por ejemplo, el tipo de no-cumplimiento o violación, mal funcionamiento actual, mensajes en la pantalla, conducta extraña);
    2) no llevar a cabo ninguna acción por cuenta propia, sino reportar inmediatamente al punto de contacto;
d) referencia a un proceso disciplinario formal establecido para tratar con los usuarios empleados, contratistas o terceros que cometen violaciones de seguridad.

En los ambientes de alto riesgo, se puede proporcionar una alarma de coacción[4] mediante la cual una persona que actúa bajo coacción puede indicar dichos problemas. Los procedimientos para responder ante las alarmas de coacción debieran reflejar la situación de alto riesgo que estas alarmas indican.

Otra información

Los ejemplos de eventos e incidentes de seguridad de la información incluyen:

a) pérdida del servicio, equipo o medios;
b) mal funcionamiento o sobre-carga del sistema;
c) errores humanos;

[4] Una alarma de coacción es un método para indicar secretamente que una acción se está realizando "bajo coacción".

d) incumplimientos de las políticas o lineamientos;
e) violaciones de los acuerdos de seguridad física;
f) cambios del sistema no controlados;
g) mal funcionamiento del software o hardware;
h) violaciones de acceso.

Con el debido cuidado a los aspectos de confidencialidad, los incidentes en la seguridad de la información pueden ser utilizados en la capacitación de los usuarios (ver 8.2.2) como ejemplos de lo que podría suceder, cómo responder ante tales incidentes y cómo evitarlos en el futuro. Para poder tratar apropiadamente los eventos e incidentes en la seguridad de la información podría ser necesario recolectar evidencia lo más pronto posible después de la ocurrencia (ver 13.2.3).

El mal funcionamiento o cualquier otra conducta anómala del sistema pueden ser un indicador de un ataque a la seguridad o una verdadera violación de la seguridad y, por lo tanto, siempre debiera reportarse como un evento en la seguridad de la información.

En ISO/IEC TR 18044 se puede encontrar más información sobre el reporte de eventos de la seguridad de la información y la gestión de incidentes de seguridad.

13.1.2 Reporte de las debilidades en la seguridad

Control

Se debiera requerir que todos los usuarios empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Lineamiento de implementación

Todos los usuarios empleados, contratistas y terceros debieran reportar estos temas ya sea a su gerencia o directamente al proveedor de su servicio lo más rápidamente posible para evitar incidentes en la seguridad de la información. El mecanismo de reporte debiera ser fácil, accesible y estar disponible lo más posible. Ellos debieran ser informados que no debieran, en ninguna circunstancia, tratar de probar una debilidad sospechada.

Otra información

Los usuarios empleados, contratistas y terceros debieran ser advertidos de no tratar de probar las debilidades de seguridad sospechadas. La prueba de las debilidades podría ser interpretada como un mal uso potencial del sistema y también podría causar daños al sistema

o servicio de información y resultar en la responsabilidad legal para la persona que realiza la prueba.

13.2 Gestión de los incidentes y mejoras en la seguridad de la información

Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información. Se debieran establecer las responsabilidades y procedimientos para manejar de manera efectivo los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debiera aplicar un proceso de mejoramiento continuo para la respuesta a, monitoreo, evaluación y la gestión general de los incidentes en la seguridad de la información. Cuando se requiera evidencia, esta se debiera recolectar cumpliendo con los requerimientos legales.

13.2.1 Responsabilidades y procedimientos

Control

Se debieran establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.

Lineamiento de la implementación

Además de reportar los eventos y debilidades en la seguridad de la información (ver también 13.1), se debiera utilizar el monitoreo del sistema, alertas y vulnerabilidades (10.10.2) para detectar los incidentes en la seguridad de la información. Se debieran considerar los siguientes lineamientos para los procedimientos de gestión de incidentes en la seguridad de la información:

a) se debieran establecer procedimientos para manejar los diferentes tipos de incidentes en la seguridad de la información, incluyendo:
   1) fallas del sistema de información y pérdida del servicio;
   2) código malicioso (ver 10.4.1);

3) negación del servicio;
4) errores resultantes de data comercial incompleta o inexacta;
5) violaciones de la confidencialidad e integridad;
6) mal uso de los sistemas de información;

b) además de los planes de contingencia normales (ver 14.1.3), los procedimientos también debieran cubrir (ver también 13.2.2):
1) análisis e identificación de la causa del incidente;
2) contención;
3) planeación e implementación de la acción correctiva para evitar la recurrencia, si fuese necesario;
4) comunicaciones con aquellos afectados por o involucrados con la recuperación de un incidente;
5) reportar la acción a la autoridad apropiada;

c) se debiera recolectar (ver 13.2.3) y asegurar rastros de auditoría y evidencia similar, conforme sea apropiado para:
1) análisis interno del problema;
2) uso como evidencia forense en relación a una violación potencial del contrato o el requerimiento regulador o en el caso de una acción legal civil o criminal; por ejemplo, bajo la legislación sobre el mal uso de computadoras o protección de data;
3) negociación para la compensación de los proveedores del software y servicio;

d) se debieran controlar formal y cuidadosamente las acciones para la recuperación de las violaciones de la seguridad y para corregir las fallas en el sistema; los procedimientos debieran asegurar que:
1) sólo el personal claramente identificado y autorizado tengan acceso a los sistemas vivos y la data (ver también 6.2 para el acceso externo);
2) se documenten en detalle todas las acciones de emergencia realizadas;
3) la acción de emergencia sea reportada a la gerencia y revisada de una manera adecuada;
4) la integridad de los sistemas y controles comerciales sea confirmada con una demora mínima.

Se debieran acordar con la gerencia los objetivos para la gestión de incidentes en la seguridad de la información, y se debieran asegurar que aquellos responsables de la gestión de incidentes en la seguridad de la información entiendan las prioridades de la organización para el manejo de los incidentes en la seguridad de la información.

Otra información

Los incidentes en la seguridad de la información podrían trascender fuera de las fronteras organizacionales y nacionales. Para responder a estos incidentes se necesita cada vez más coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas, conforme sea apropiado.

13.2.2 Aprender de los incidentes en la seguridad de la información

Control

Se debieran establecer mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.

Lineamiento de implementación

Se debiera utilizar la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Otra información

La evaluación de los incidentes en la seguridad de la información pueden indicar la necesidad de incrementar o establecer controles adicionales para limitar la frecuencia, daño y costo de ocurrencias futuras, o tomarlos en cuenta en el proceso de revisión de la política de seguridad (ver 5.1.2).

13.2.3 Recolección de evidencia

Control

Cuando una acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (ya sea civil o criminal); se debiera recolectar, mantener y presentar evidencia para cumplir con las reglas de evidencia establecidas en la(s) jurisdicción(es) relevante(s).

Lineamiento de implementación

Se debieran desarrollar y seguir los procedimientos internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización.

En general, las reglas de evidencia debieran abarcar:

a) admisibilidad de la evidencia: si la evidencia se puede o no se puede utilizar en la corte;
b) peso de la evidencia: la calidad e integridad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debiera asegurar que sus sistemas de información cumplan con todos los estándares o códigos de práctica publicados para la producción de evidencia admisible.

El peso de la evidencia provisto debiera cumplir con cualquier requerimiento aplicable. Para lograr el peso de la evidencia, se debiera demostrar mediante un rastro de auditoría sólido la calidad y la integridad de los controles utilizados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) durante todo el período en que la evidencia a ser recuperada fue almacenada y procesada. Este rastro de auditoría sólido se puede establecer bajo las siguientes condiciones:

a) para los documentos en papel: el original se debiera mantener de manera segura con un registro de la persona quien encontró el documento, el lugar donde se encontró el documento, cuándo se encontró el documento y quién presenció el descubrimiento; cualquier investigación debiera asegurar que no se alteren o manipulen los originales;

b) para la información en medios de cómputo: se debieran realizar imágenes dobles o copias (dependiendo de los requerimientos aplicables) de cualquier medio e información en discos duros o en memoria para asegurar su disponibilidad; se debiera mantener un registro de todas las acciones realizadas durante el proceso de copiado y el proceso debiera ser atestiguado; el medio original y el registro (si esto no es posible, por lo menos una imagen doble o una copia) se debieran mantener de manera segura y sin ser tocados.

Cualquier trabajo forense sólo se debiera realizar en las copias del material de evidencia. Se debiera proteger la integridad de todo el material de evidencia. El copiado del material de evidencia debiera ser supervisado por personal confiable y se debiera registrar la información sobre cuándo y dónde se realiza el proceso de copiado, quién realiza las actividades de copiado y cuáles herramientas y programas se han utilizado.

Otra información

Cuando recién se detecta un evento en la seguridad de la información, puede no ser obvio si el evento resultará, o no, en una acción legal. Por lo tanto, existe el peligro que la evidencia necesaria sea destruida involuntaria o accidentalmente antes de percatarse de la seriedad del incidente. Es aconsejable involucrar a un abogado o la policía desde el inicio de una acción legal contemplada y tomar asesoría sobre la evidencia requerida.

La evidencia puede trascender las fronteras organizacionales y/o jurisdiccionales. En tales casos, se debiera asegurar que la organización tenga el derecho de recolectar la información

requerida como evidencia. Se debieran considerar los requerimientos de las diferentes jurisdicciones para maximizar las posibilidades de admisión a través de las jurisdicciones relevantes.

14 Gestión de la continuidad del negocio

14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

Objetivo: Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Se debiera implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debiera identificar los procesos comerciales críticos e integrar los requerimientos de gestión de la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios.

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se debieran desarrollar e implementar planes para la continuidad del negocio para asegurar la reinundación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

La gestión de la continuidad del negocio debiera incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales.

14.1.1 Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio

Control

Se debiera desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

Lineamiento de implementación

El proceso debiera reunir los siguientes elementos claves de la gestión de continuidad del negocio:

a) entender los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y priorización de los procesos comerciales críticos (ver 14.1.2)
b) identificar todos los activos involucrados en los procesos comerciales críticos (ver 7.1.1);
c) entender el impacto que probablemente tendrán las interrupciones causadas por incidentes en la seguridad de la información en el negocio (es importante encontrar las soluciones que manejen los incidentes que causan el menor impacto, así como los incidentes serios que pueden amenazar la viabilidad de la organización), y establecer los objetivos comerciales de los medios de procesamiento de la información;
d) considerar la compra de un seguro adecuado que pueda formar parte de un proceso general de la continuidad del negocio, y que también sea parte de la gestión del riesgo operacional;
e) identificar y considerar la implementación de controles preventivos y atenuantes adicionales;
f) identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requerimientos de seguridad de la información identificados;
g) garantizar la seguridad del personal y la protección de los medios de procesamiento de la información y la propiedad organizacional;
h) formular y documentar los planes de continuidad del negocio tratando los requerimientos de seguridad de la información en línea con la estrategia acordada para la continuidad del negocio (ver 14.1.3);
i) pruebas y actualizaciones regulares de los planes y procesos (ver 14.1.5);
j) asegurar que la gestión de la continuidad del negocio se incorpore a los procesos y estructura de la organización; se debiera asignar la responsabilidad del proceso de la gestión de la continuidad del negocio en el nivel apropiado dentro de la organización (ver 6.1.1).

14.1.2 Continuidad del negocio y evaluación del riesgo

Control

Se debieran identificar los eventos que pueden causar interrupciones a los procesos comerciales, junto con la probabilidad y el impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.

Lineamiento de implementación

Los aspectos de la seguridad de la información de la continuidad del negocio se debieran basar en la identificación de los eventos (o secuencia de eventos) que pueden causar las interrupciones en los procesos comerciales de la organización; por ejemplo, fallas en el equipo, errores humanos, robo, fuego, desastres naturales y actos de terrorismo. Esto debiera ir seguido por una evaluación del riesgo para determinar la probabilidad e impacto de dichas interrupciones, en términos de tiempo, escala del daño y período de recuperación.

La evaluación del riesgo de la continuidad el negocio se debiera llevar a cabo con la participación total de los propietarios de los recursos y procesos comerciales. Esta evaluación debiera considerar los procedimientos comerciales y no se debieran limitar a los medios de procesamiento de la información, y debieran incluir los resultados específicos para la seguridad de la información. Es importante vincular los diferentes aspectos del riesgo para obtener una imagen completa de los requerimientos de continuidad comercial de la organización. La evaluación debiera identificar, cuantificar y priorizar los riesgos en comparación con los criterios y objetivos relevantes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, tiempos de desabastecimiento permitidos y prioridades de recuperación.

Dependiendo de los resultados de la evaluación del riesgo, se debiera desarrollar una estrategia de continuidad del negocio para determinar el enfoque general para la continuidad del negocio. Una vez que se ha creado la estrategia, la gerencia debiera proporcionarle su respaldo, y crear y respaldar un plan para implementar esta estrategia.

14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información

Control

Se debieran desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos.

Lineamiento de implementación

El proceso de planeación de la continuidad del negocio debiera considerar lo siguiente:

a) identificar y acordar todas las responsabilidades y los procedimientos de continuidad del negocio;
b) identificar la pérdida aceptable de la información y los servicios;
c) implementación de los procedimientos para permitir la recuperación y restauración de las operaciones comerciales y la disponibilidad de la información en las escalas de tiempo requeridas; se debiera prestar particular atención a la evaluación de las dependencias comerciales internas y externas y el establecimiento de los contratos debidos;
d) los procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración;
e) documentación de los procesos y procedimientos acordados;
f) educación apropiada del personal en los procedimientos y procesos acordados, incluyendo la gestión de crisis;
g) prueba y actualización de los planes.

El proceso de planeación debiera enfocarse en los objetivos comerciales requeridos; por ejemplo, restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable. Se debieran identificar los servicios y los recursos que facilitan esto; incluyendo personal, recursos de procesamiento no-información; así como los arreglos de contingencia para los medios de procesamiento de información. Estos arreglos de contingencia pueden incluir acuerdos con terceros en la forma de acuerdos recíprocos, o servicios de suscripción comercial.

Los planes de continuidad del negocio debieran tratar las vulnerabilidades organizacionales y, por lo tanto, pueden contener información confidencial que necesita protegerse apropiadamente. Las copias de los planes de continuidad del negocio se debieran almacenar en locales remotos, a una distancia suficiente para escapar de cualquier daño de un desastre en el local principal. La gerencia debiera asegurarse que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el local principal. Otro material necesario para ejecutar los planes de continuidad también debiera almacenarse en el local remoto.

Si se utilizan ubicaciones temporales alternativas, el nivel de los controles de seguridad implementados en esos locales debiera ser equivalente al de los controles del local principal.

Otra información

Se debiera notar que estos planes y actividades de gestión de crisis (ver 14.1.3f) pueden ser diferentes a los de la gestión de la continuidad del negocio; es decir, puede ocurrir una crisis que puede ser acomodada por los procedimientos gerenciales normales.

14.1.4 Marco Referencial de la planeación de la continuidad del negocio

Control

Se debiera mantener un solo marco referencial de los planes de continuidad del negocio para asegurar que todos los planes sean consistentes, tratar consistentemente los requerimientos de seguridad de la información e identificar las prioridades para la prueba y el mantenimiento.

Lineamiento de implementación

Cada plan de continuidad comercial describe el enfoque para la continuidad, por ejemplo el enfoque para asegurar la disponibilidad y seguridad de la información o sistema de información. Cada plan también debiera especificar el plan de intensificación y las condiciones para la activación, así como las personas responsables de ejecutar cada componente del plan. Con los nuevos requerimientos identificados, cualquier procedimiento de emergencia existente; por ejemplo, los planes de evacuación o arreglos de emergencia; debiera ser enmendado conforme sea apropiado. Los procedimientos debieran incluirse dentro del programa de gestión de cambio de la organización para asegurar que los ítems de continuidad del negocio siempre sean tratados apropiadamente.

Cada plan debiera tener un propietario específico. Los procedimientos de emergencia, planes de contingencia manuales y planes de reanudación debieran estar dentro de la responsabilidad del propietario de los recursos o procesos comerciales apropiados involucrados. Los arreglos de contingencia para los servicios técnicos alternativos, como los medios de procesamiento de la información y comunicaciones, usualmente debieran ser responsabilidad de los proveedores del servicio.

Un marco de planeación de continuidad del negocio debiera tratar los requerimientos de seguridad de la información y considerar lo siguiente:

a) las condiciones para activar los planes que describen el proceso a seguirse (por ejemplo, cómo evaluar la situación, quién va a participar) antes de activar cada plan;
b) los procedimientos de emergencia que describen las acciones a realizarse después del incidente que pone en riesgo las operaciones comerciales;
c) procedimientos de contingencia que describen las acciones tomadas para trasladar las actividades comerciales esenciales de los servicios de soporte a locales

temporales alternativos, y regresar los procesos comerciales a la operación en las escalas de tiempo requeridas;

d) procedimientos operacionales temporales a seguirse hasta la culminación de la recuperación y restauración;
e) procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales;
f) un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan;
g) las actividades de conciencia, educación y capacitación diseñadas para crear el entendimiento de los procesos de continuidad del negocio y asegurar que los procesos continúen siendo efectivos;
h) las responsabilidades de las personas, describiendo quién es el responsable de ejecutar cuál componente del plan. Se debieran nombrar alternativas conforme sea necesario.
i) los activos y recursos críticos necesitan ser capaces de realizar los procedimientos de emergencia, de respaldo y reanudación.

14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio

Control

Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.

Lineamiento de implementación

Las pruebas del plan de continuidad del negocio debieran asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén al tanto de los planes y su responsabilidad con la continuidad del negocio y la seguridad de la información, y que conozcan su papel cuando se invoque el plan.

El programa de pruebas para el(los) plan(es) de continuidad debieran indicar cómo y cuándo se debiera probar cada elemento del plan. Cada elemento del(los) plan(es) debiera(n) ser probado(s) frecuentemente:

a) prueba flexible de simulación (table-top testing) de varios escenarios (discutiendo los acuerdos de recuperación comercial utilizando ejemplos de interrupciones);
b) simulaciones (particularmente para capacitar a las personas en sus papeles en la gestión post-incidente/crisis);
c) prueba de recuperación técnica (asegurando que los sistemas de información puedan restaurarse de manera efectiva;

d) prueba de recuperación en el local alternativo (corriendo los procesos comerciales en paralelo con las operaciones de recuperación lejos del local principal);
e) pruebas de los medios y servicios del proveedor (asegurando que los servicios y productos provistos externamente cumplan con el compromiso contraído);
f) ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).

Estas técnicas se pueden utilizar en cualquier organización. Esto se debiera aplicar de una manera que sea relevante para el plan de recuperación específico. Los resultados de las pruebas debieran ser registradas y, cuando sea necesario, se debieran tomar acciones para mejorar los planes.

Se debiera asignar la responsabilidad de las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en los acuerdos comerciales que aún no se reflejan en los planes de continuidad del negocio debiera realizarse mediante una actualización apropiada del plan. Este proceso formal de control de cambios debiera asegurar que los planes de actualización sean distribuidos y reforzados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios que se debieran considerar cuando se actualizan los planes de continuidad del negocio son la adquisición de equipo nuevo, actualización de los sistemas y cambios en:

a) personal;
b) direcciones o números de teléfonos;
c) estrategia comercial;
d) local, medios y recursos;
e) legislación;
f) contratistas, proveedores y clientes claves;
g) procesos, los nuevos o los eliminados;
h) riesgo (operacional y funcional).

15 Cumplimiento

15.1 Cumplimiento de los requerimientos legales

Objetivo: Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad. El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales. Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de data inter-fronteras).

15.1.1 Identificación de la legislación aplicable

Control

Se debiera definir explícitamente, documentar y actualizar todos los requerimientos estatutarios, reguladores y contractuales relevantes, y el enfoque de la organización para satisfacer esos requerimientos, para cada sistema de información y la organización.

Lineamiento de implementación

Similarmente, se debieran definir y documentar los controles y responsabilidades individuales específicos para satisfacer estos requerimientos.

15.1.2 Derechos de propiedad intelectual (IPR)

Control

Se debieran implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para proteger cualquier material que se considere de propiedad intelectual:

a) una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos de software e información;
b) sólo adquirir software a través de fuentes conocidos y acreditados para asegurar que no sean violados los derechos de autor;
c) mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual, y notificar de la voluntad de tomar una acción disciplinaria contra el personal que los viole;
d) monitorear los registros de activos apropiados, e identificar todos los activos con los requerimientos para proteger los derechos de propiedad intelectual;
e) mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.
f) implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos;
g) llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia;
h) proporcionar una política para mantener las condiciones de licencias apropiadas;
i) proporcionar una política para eliminar o transferir el software a otros;
j) utilizar las herramientas de auditoria apropiadas;
k) cumplir con los términos y condiciones del software e información obtenida de redes públicas;
l) no duplicar, convertir a otro formato o extraer de registros comerciales (audio, vídeo), aparte de los permitidos por la ley de derechos de autor;
m) no copiar; completamente o en parte; libros, artículos, reportes u otros documentos; aparte de aquellos permitidos por la ley de derechos de autor.

Otra información

Los derechos de propiedad intelectual incluyen los derechos de autor, derechos de diseño, marcas registradas, patentes y licencias de código fuente de software o documentos.

Los productos de software patentados usualmente son suministrados mediante un contrato de licencia que especifica los términos y condiciones de las licencias, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando el copiado sólo a la creación de copias de respaldo. Se necesita aclarar la situación IPR del software desarrollado por la organización con el personal.

Los requerimientos legislativos, reguladores y contractuales pueden colocar restricciones sobre el copiado de material patentado. En particular, ellos pueden requerir que sólo se pueda utilizar el material desarrollado por la organización, o que sea licenciado o provisto por un

diseñador a la organización. La violación de los derechos de autor puede llevar a una acción legal, lo cual puede involucrar los trámites judiciales.

15.1.3 Protección de registros organizacionales

Control

Se debieran proteger los registros importantes de pérdida, destrucción, falsificación; en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.

Lineamiento de implementación

Los registros debieran ser clasificados en tipos de registros; por ejemplo; registros de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operacionales; cada uno con detalles de los períodos de retención y el tipo de medio de almacenaje; por ejemplo, papel, microficha, magnético, óptico. Cualquier material criptográfico y programas asociados con los archivos codificados o firmas digitales (ver 12.3) también debieran ser almacenados para permitir la descripción de los registros durante el tiempo que se mantengan los archivos.

Se debiera tener en consideración la posibilidad del deterioro de los medios utilizados para el almacenaje de registros. Se debieran implementar los procedimientos de almacenaje y manipuleo en concordancia con las recomendaciones del fabricante. Para el almacenaje a largo plazo, se debiera considerar el uso de papel y microfichas.

Cuando se eligen medios de almacenaje electrónicos, se debiera incluir los procedimientos para asegurar la capacidad de acceso a la data (medios y formato de lectura) durante todo el período de retención, para salvaguardarlos de la pérdida causada por un futuro cambio en la tecnología.

Se debiera elegir los sistemas de almacenaje de data de manera que la data pueda ser recuperada en un marco de tiempo y formato aceptable, dependiendo de los requerimientos que se debieran cumplir.

El sistema de almacenaje y manipuleo debiera asegurar la identificación clara de los registros y de su período de retención tal como lo definen la legislación o las regulaciones nacionales o regionales, si fuesen aplicables. Este sistema debiera permitir la apropiada destrucción de los registros después de un período adecuado si es que ya no son necesarios para la organización.

Para satisfacer estos objetivos de protección de registros, se debieran tomar los siguientes pasos dentro de una organización:

a) se debieran emitir lineamientos sobre la retención, almacenaje, manipuleo y eliminación de registros e información;
b) se debiera diseñar un programa de retención para identificar los registros y el período de tiempo durante el cual se debieran retener;
c) se debiera mantener un inventario de fuentes de información clave;
d) se debieran implementar los controles apropiados para proteger los registros y la información de pérdida, destrucción y falsificación.

Otra información

Algunos registros pueden necesitar ser mantenidos de forma segura para cumplir con requerimientos estatutarios, reguladores o contractuales; así como para respaldar las actividades comerciales esenciales. Los ejemplos incluyen registros que pueden ser requeridos como evidencia de que una organización opera dentro de las reglas estatutarias o reguladoras, para asegurar la defensa adecuada contra una potencial acción civil o criminal, o para confirmar el estado financiero de una organización con respecto a los accionistas, partes externas y auditores. El período de tiempo y el contenido de la data para la retención de la información se pueden establecer mediante la regulación o ley nacional.

Se puede encontrar más información sobre el manejo de los registros organizacionales en ISO 15489-1.

15.1.4 Protección de la data y privacidad de la información personal

Control

Se debiera asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

Lineamiento de implementación

Se debiera desarrollar e implementar una política de protección y privacidad de la data. Esta política debiera ser comunicada a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y toda legislación y regulación de protección de data relevante requiere una apropiada estructura y control gerencial. Con frecuencia esto se logra asignando a una persona como responsable, por ejemplo un funcionario de protección de data, quien debiera proporcionar lineamientos a los gerentes, usuarios y proveedores de los servicios

sobre sus responsabilidades individuales y los procedimientos específicos que debieran seguir. La responsabilidad por el manejo de la información personal y el reforzamiento del conocimiento de los principios de protección de data debieran ser tratados en concordancia con la legislación y las regulaciones relevantes. Se debieran implementar las apropiadas medidas técnicas y organizacionales para protección la información personal.

Otra información

Un número de países han introducido una legislación colocando controles sobre la recolección, procesamiento y transmisión de data personal (generalmente la información sobre personas vivas que pueden ser identificadas mediante esa información). Dependiendo de la legislación nacional respectiva, dichos controles pueden imponer impuestos a aquellos que recolectan, procesan y difunden información personal; y pueden restringir la capacidad para transferir la data a otros países.

15.1.5 Prevención del mal uso de los medios de procesamiento de la información

Control

Se debiera disuadir a los usuarios de utilizar los medios de procesamiento de la información para propósitos no autorizados.

Lineamiento de implementación

La gerencia debiera aprobar el uso de los medios de procesamiento de la información. Cualquier uso de estos medios para propósitos no-comerciales sin aprobación de la gerencia (ver 6.1.4), o para cualquier propósito no autorizado, será visto como un uso inapropiado de los medios. Si mediante el monitoreo, o cualquier otro medio, se identifica una actividad no autorizada, esta actividad debiera ser puesta en atención del gerente a cargo para que considere la acción disciplinaria y/o legal apropiada.

Se debiera contar con asesoría legal antes de la implementación de los procedimientos de monitoreo.

Todos los usuarios debieran estar al tanto del alcance preciso que su acceso permitido y del monitoreo establecido para detectar el uso no autorizado. Esto se puede lograr danto a los usuarios una autorización escrita, debiendo uno copia estar firmada por el usuario y ser mantenida de manera segura por la organización. Los empleados de una organización, contratistas y terceros debieran estar advertidos que no se permitirá ningún acceso excepto de aquel que fue autorizado.

A la hora del registro, se debiera presentar un mensaje para indicar que al medio que procesamiento de información al cual se está ingresando es propiedad de la organización y no está permitido ningún acceso no autorizado. El usuario tiene que conocer y reaccionar apropiadamente al mensaje en la pantalla para continuar con el proceso de registro (ver 11.5.1).

Otra información

Los medios de procesamiento de la información de una organización están diseñados principal o exclusivamente para propósitos comerciales.

La detección de intrusiones, inspección de contenido y otras herramientas de monitoreo pueden ayudar a evitar y detectar el mal uso de los medios de información.

Muchos países tienen una legislación para proteger el mal uso de los medios de cómputo. Puede ser una ofensa criminal utilizar una computadora para propósitos no autorizados.

La legalidad del monitoreo de la utilización varía de país en país, y puede requerir que la gerencia advierta a todos los usuarios de tal monitoreo y/o obtener su consentimiento. Cuando el sistema al cual se ingresa se utiliza para el acceso público (por ejemplo, un servidor de web público), y está sujeto al monitoreo de seguridad, se debiera mostrar un mensaje advirtiéndolo.

15.1.6 Regulación de controles criptográficos

Control

Los controles criptográficos se debieran utilizar en cumplimiento con todos los acuerdos, leyes y regulaciones relevantes.

Lineamiento de implementación

Se debieran considerar los siguientes ítems para el cumplimiento con los acuerdos, leyes y regulaciones relevantes:

a) las restricciones sobre la importación y/o exportación de hardware y software de cómputo para realizar funciones criptográficas;
b) las restricciones sobre la importación y/o exportación de hardware y software de cómputo diseñado para agregarle funciones criptográficas;
c) restricciones sobre la utilización de la codificación;
d) métodos obligatorios o voluntarios para que las autoridades de los países tengan acceso a la información codificada por hardware o software para proporcionar confidencialidad del contenido.

Se debiera buscar asesoría legal para asegurar el cumplimiento de las leyes y regulaciones nacionales. Antes que la información codificada o los controles criptográficos sean trasladados a otro país, se debiera buscar asesoría legal.

15.2 Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional. La seguridad de los sistemas de información se debiera revisar regularmente. Estas revisiones debieran realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información debieran ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

15.2.1 Cumplimiento con las políticas y estándares de seguridad

Control

Los gerentes debieran asegurar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad para asegurar el cumplimiento de las políticas y estándares de seguridad.

Lineamiento de implementación

Los gerentes debieran revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas y estándares de seguridad apropiados, y cualquier otro requerimiento de seguridad.

Si se encuentra cualquier incumplimiento como resultado de la revisión, los gerentes debieran:

a) determinar las causas del incumplimiento;

b) evaluar la necesidad de acciones para asegurar que no vuelva a ocurrir el incumplimiento;
c) determinar e implementar la acción correctiva apropiada;
d) revisar la acción correctiva tomada.

Los resultados de las revisiones y las acciones correctivas tomadas por los gerentes debieran ser registrados y se debieran mantener estos registros. Cuando se lleva a cabo una revisión independiente en el área de su responsabilidad, los gerentes debieran reportar los resultados a la persona que está llevando a cabo las revisiones independientes (ver 6.1.8).

Otra información

El monitoreo operacional del uso del sistema se trata en el 10.10.

15.2.2 Chequeo del cumplimiento técnico

Control

Los sistemas de información debieran chequearse regularmente para ver el cumplimiento de los estándares de implementación de la seguridad.

Lineamiento de implementación

El chequeo del cumplimiento técnico debiera ser realizado manualmente (respaldado por las herramientas de software apropiadas, si fuese necesario) por un ingeniero de sistemas experimentado y/o con la asistencia de herramientas automatizadas, las cuales generan un reporte técnico para su subsiguiente interpretación por un especialista técnico.

Si se utilizan pruebas de penetración o evaluaciones de vulnerabilidad, se debiera tener cuidado ya que estas actividades pueden llevar a comprometer la seguridad del sistema. Estas pruebas se debieran planear, documentar y repetir.

Todo chequeo de cumplimiento técnico debiera ser llevado a cabo por personas autorizadas y competentes, o bajo la supervisión de estas personas.

Otra información

El chequeo del cumplimiento técnico involucra el examen de los sistemas operacionales para asegurar que los controles de hardware y software se hayan implementado correctamente. Este tipo de chequeo del cumplimiento requiere de una experiencia técnica especializada.

El chequeo del cumplimiento también abarca, por ejemplo, una prueba de penetración y evaluación de vulnerabilidades, las cuales se podrían llevar a cabo por expertos

independientes contratados específicamente para ese propósito. Esto puede ser útil para detectar vulnerabilidades en el sistema y para chequear la efectividad de los controles para evitar un acceso no autorizado debido a estas vulnerabilidades.

La prueba de penetración y la evaluación de vulnerabilidades proporcionan una imagen de un sistema en un estado específico en un momento específico. La imagen se limita a esas partes del sistema probadas durante el(los) intento(s) de penetración. La prueba de penetración y las evaluaciones de vulnerabilidades no son un sustituto de la evaluación del riesgo.

15.3 Consideraciones de auditoria de los sistemas de información

Objetivo: Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información. Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría. También se requiere protección para salvaguardar la integridad y evitar el mal uso de las herramientas de auditoría.

15.3.1 Controles de auditoría de los sistemas de información

Control

Las actividades y requerimientos de auditoría que involucran chequeos de los sistemas operacionales debieran ser planeados y acordados cuidadosamente para minimizar el riesgo de interrupciones en los procesos comerciales.

Lineamiento de implementación

Se debieran observar los siguientes lineamientos:

a) se debieran acordar los requerimientos de auditoría con la gerencia apropiada;

b) se debiera acordar y controlar el alcance de los chequeos;

c) los chequeos debieran limitarse a un acceso sólo-de-lectura al software y data;

d) sólo se debiera permitir un acceso diferente al sólo-de-lectura para copias aisladas de los archivos del sistema, los cuales se pueden borrar cuando termina la auditoría, o se les puede dar la protección apropiada si existe la obligación de mantener dichos archivos en concordancia con los requerimientos de la documentación de auditoría;

e) se debieran identificar explícitamente los recursos para realizar los chequeos y debieran estar disponibles;

f) se debieran identificar y acordar los requerimientos de procesamiento especial o adicional;

g) se debieran monitorear y registrar todos los accesos para producir un rastro de referencia; se debiera considerar el uso de rastros de referencia con la hora impresa para la data o sistemas críticos;

h) se debieran documentar todos los procedimientos, requerimientos y responsabilidades;

i) la(s) personas(s) que llevan a cabo la auditoría debieran ser independientes a las actividades auditadas.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control

Se debiera proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o trasgresión posible.

Lineamiento de implementación

Las herramientas de auditoría de los sistemas de información; por ejemplo, software o archivos de data; debieran estar separadas de los sistemas de desarrollo y operacionales y no se debieran mantener en las bibliotecas de cintas o áreas de usuario, a no ser que se les proporcione un nivel apropiado de protección adicional.

Otra información

Si terceras personas participan en la auditoría, puede existir el riesgo que estas terceras personas hagan un mal uso de las herramientas de auditoría y que la organización de estas terceras personas tenga acceso a la información. Se pueden considerar los controles tales como el 6.2.1 (para evaluar los riesgos) y 9.1.2 (para restringir el acceso físico) para tratar este riesgo, y se debiera realizar cualquier acción consecuente, como el cambio inmediato de las claves secretas proporcionadas a los auditores.

Bibliografía

ISO/IEC Guía 2:1996, Estandarización y actividades relacionadas – Vocabulario General

ISO/IEC Guía 73:2002, Gestión del riesgo – Vocabulario – Lineamientos para el uso en estándares

ISO/IEC 13335-1:2004, Tecnología de la información –Técnicas de seguridad – Gestión de la seguridad en la tecnología de la información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de la seguridad de la tecnología de la información y comunicaciones

ISO/IEC TR 13335-3:1998, Tecnología de la información – Lineamientos para la Gestión de la Seguridad TI – Parte 3: Técnicas para la gestión de la Seguridad TI

ISO/IEC 13888-1:1997, Tecnología de la Información – Técnicas de seguridad – No Repudio – Parte 1: General

ISO/IEC 11770-1:1996 Tecnología de la información – Técnicas de seguridad – Gestión clave – Parte 1: Marco Referencial

ISO/IEC 9796:2002 Tecnología de la información – Técnicas de seguridad – Esquemas de firmas digitales dando recuperación del mensaje – Parte 2: Factorización en números enteros basado en mecanismos

ISO/IEC 9796-3:2000 Tecnología de la información – Técnicas de seguridad - Esquemas de firmas digitales dando recuperación del mensaje – Parte 3: Logaritmo discreto basado en mecanismos

ISO/IEC 14888-1:1998 Tecnología de la información – Técnicas de seguridad – Firmas digitales con apéndice – Parte 1: General

ISO/IEC 15408-1:1999 Tecnología de la información – Técnicas de seguridad – Criterios de Evaluación para la seguridad TI – Parte 1: Introducción y modelo general

ISO/IEC 14516:2002 Tecnología de la información – Técnicas de seguridad – Lineamientos para el uso y gestión de los servicios de Terceras Personas Confiables

ISO 15489-1:2001 Información y documentación – Gestión de registros – Parte 1: General

ISO 10007:2003 Sistemas de gestión de calidad – Lineamientos para la gestión de la configuración

ISO/IEC 12207:1995 Tecnología de la información – Procesos del ciclo de vida del software

ISO 19011:2002 Lineamientos para la auditoría de sistemas de gestión de calidad y/o ambiental

OECD Lineamientos para la Seguridad de Sistemas de Información y Redes: "hacia una Cultura de Seguridad", 2002

OECD Lineamientos para la Política de Criptografía, 1997

IEEE P1363-2000: Especificaciones Estándar para la Criptografía de Claves Públicas

ISO/IEC 18028-4 Tecnología de la información –Técnicas de seguridad – Seguridad de Red TI – Parte 4: Asegurando el acceso remoto

ISO/IEC TR 18044 Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información

Índice