NORMA CHILENA NCh-ISO 27002

Segunda edición
2013.10.25

Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información

Information technology - Security techniques - Code of practice for information security controls

Número de referencia
NCh-ISO 27002:2013

DOCUMENTO PROTEGIDO POR COPYRIGHT

Instituto Nacional de Normalización - INN
Matías Cousiño 64, piso 6 • Santiago de Chile
Tel. + 56 2 445 88 00
Fax + 56 2 441 04 29
Correo Electrónico info@inn.cl
Sitio Web www.inn.cl
Publicado en Chile

Contenido

Página

Contenido

Página

Tecnologías de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información

Preámbulo

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

Esta norma se estudió por el Comité Técnico *Conjunto de caracteres y codificación*, y brinda orientación para las normas de seguridad de información organizacional y las prácticas de administración de seguridad de la información incluida la selección, la implementación, la administración y los controles considerando los entornos de riesgo de seguridad de la información de la organización

Esta norma es idéntica a la versión en inglés de la Norma ISO/IEC 27002:2013 *Information technology - Security techniques - Code of practice for information security controls.*

La Nota Explicativa incluida en un recuadro en cláusula 2 Referencias normativas y Anexo A Bibliografía, es un cambio editorial que se incluye con el propósito de informar la correspondencia con Norma Chilena de las Normas Internacionales citadas en esta de norma.

Para los propósitos de esta norma, se han realizado los cambios editoriales que se indican y justifican en Anexo B.

Los Anexos A y B no forman parte de la norma, se insertan sólo a título informativo.

Si bien se ha tomado todo el cuidado razonable en la preparación y revisión de los documentos normativos producto de la presente comercialización, INN no garantiza que el contenido del documento es actualizado o exacto o que el documento será adecuado para los fines esperados por el cliente.

En la medida permitida por la legislación aplicable, el INN no es responsable de ningún daño directo, indirecto, punitivo, incidental, especial, consecuencial o cualquier daño que surja o esté conectado con el uso o el uso indebido de este documento.

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 25 de octubre de 2013.

Tecnologías de la información -Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información

0 Introducción

0.1 Alcance y contexto

Esta norma está diseñada para que las organizaciones la utilicen como referencia al seleccionar los controles dentro del proceso para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en base a ISO/IEC 27001 o como un documento de orientación para las organizaciones que implementan controles de seguridad de información de aceptación común. Esta norma también está hecha para utilizarse en el desarrollo de pautas de administración de seguridad de la industria y específicas para la organización, considerando sus entornos específicos de riesgo de seguridad de la información.

Las organizaciones de todos los tipos y tamaños (incluido el sector público y privado, comercial y sin fines de lucro) recopilan, procesan y transmiten información de varias formas incluidas las electrónicas, físicas y verbales (es decir, conversaciones y presentaciones).

El valor de la información traspasa las palabras escritas, los números y las imágenes: el conocimiento, los conceptos, las ideas y las marcas son ejemplos de formas intangibles de información. En un mundo interconectado, la información y los procesos relacionados, los sistemas, redes y el personal involucrado en su operación, manipulación y protección son activos que, al igual que otros activos comerciales de importancia, resultan valiosos para el negocio de la organización y, por lo tanto, merecen o requieren protección contra diversos peligros.

Los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos, sistemas, redes y personas relacionadas poseen vulnerabilidades inherentes. Los cambios en los procesos y sistemas comerciales u otros cambios externos (como las nuevas leyes y normativas) pueden generar nuevos riesgos para la seguridad de la información. Por lo tanto, dada la multitud de formas en que las amenazas se pueden aprovechar de las vulnerabilidades para dañar a la organización, los riesgos en la seguridad de la información siempre están presentes. La seguridad eficaz en la información reduce estos riesgos al proteger a la organización contra las amenazas y vulnerabilidades y luego reduce el impacto en sus activos.

La seguridad de la información se logra implementando un conjunto de controles adecuado, que incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Estos controles se deberían establecer, implementar, monitorear, revisar y mejorar donde sea necesario para garantizar que se cumplen los objetivos específicos comerciales y de seguridad de las organizaciones. Un SGSI como el que se especifica en ISO/IEC 27001 toma un punto de vista holístico y coordinado de los riesgos de seguridad de la información de la organización para poder implementar una suite integral de controles de seguridad de la información bajo el marco general completo de un sistema de administración coherente.

Muchos sistemas de información no se han diseñado para ser seguros en el aspecto de ISO/IEC 27001 y esta norma. La seguridad que se puede lograr a través de medios técnicos es limitada y debería estar respaldada por la administración y procedimientos adecuados. La identificación de los controles que se deberían poner en vigencia requiere de una planificación minuciosa y detallada. Un SGSI correcto requiere del apoyo de todos los empleados de la organización. También puede requerir la participación de accionistas, proveedores y otras partes externas. También es posible que se necesite asesoría de especialistas de partes externas.

En un sentido más amplio, la seguridad de la información eficaz también garantiza a la dirección y a otras partes interesadas que los activos de la organización se encuentran razonablemente seguros y protegidos contra daños y, por lo tanto, que actúan como una herramienta de apoyo para el negocio.

0.2 Requisitos de la seguridad de la información

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

a) la evaluación de los riesgos para la organización, considerando la estrategia y los objetivos generales de la organización. Las amenazas a los activos se identifican a través de una evaluación de riesgos, se evalúa además la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto;

b) los requisitos legales, estatutarios, normativos y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicio deberían satisfacer y su entorno sociocultural;

c) el conjunto de principios, objetivos y requisitos comerciales para el manejo, el procesamiento, el almacenamiento, la comunicación y el archivado de la información que ha desarrollado una empresa para apoyar a sus operaciones.

Los recursos empleados en la implementación de controles se deberían equilibrar contra el probable daño al negocio que puede surgir de los problemas de seguridad en la ausencia de estos controles. Los resultados de una evaluación de riesgos ayudarán a guiar y determinar las acciones y prioridades de gestión adecuadas para administrar los riesgos de seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos.

La norma ISO/IEC 27005 proporciona orientación sobre la administración de riesgos de seguridad de la información e incluye datos sobre la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos, la comunicación de riesgos, el monitoreo de riesgos y la revisión de riesgos.

0.3 Selección de controles

Los controles se pueden seleccionar a partir de esta norma o de otros conjuntos de controles, o bien se pueden diseñar nuevos controles para cumplir con las necesidades específicas según sea necesario.

La selección de los controles depende de las decisiones organizacionales en base a los criterios para la aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque de administración general de riesgos que se aplica a la organización y también estará sujeta a toda la legislación y normativas nacionales e internacionales pertinentes. La selección del control también depende de la forma en que interactúan los controles para brindar protección en profundidad.

Algunos de los controles de esta norma se pueden considerar como principios guía para la administración de la seguridad de la información y se pueden aplicar a la mayoría de las organizaciones. Los controles se explican en mayor detalle a continuación junto con la orientación sobre la implementación. Puede encontrar más información sobre la selección de controles y opciones de tratamiento de riesgos en ISO/IEC 27005.

0.4 Desarrollo de sus propias pautas

Esta norma se puede considerar como un punto de partida para desarrollar pautas específicas para la organización. Es posible que no todos los controles y pautas de este código de prácticas se puedan aplicar. Más aún, es posible que se requieran controles y pautas adicionales que no se incluyen en esta norma. Cuando los documentos se desarrollan conteniendo pautas o controles adicionales, puede resultar útil incluir referencias cruzadas a las cláusulas en esta norma donde corresponda para facilitar la comprobación del cumplimiento por parte de los auditores y los socios comerciales.

0.5 Consideraciones sobre el ciclo de vida

La información tiene un ciclo de vida natural, desde la creación y el origen, pasando por el almacenamiento, el procesamiento, el uso y la transmisión, hasta su eventual destrucción o decaimiento. El valor y los riesgos a los activos puede variar a lo largo de su vida útil (es decir, la divulgación no autorizada o robo de las cuentas financieras de una empresa es mucho menos importante después de que se han publicado formalmente), pero la seguridad de la información sigue siendo importante en cierta medida en todas las etapas.

Los sistemas de información tienen ciclos de vida dentro de los que se conciben, especifican, diseñan, desarrollan, prueban, implementan, utilizan, mantienen y que con el tiempo se retiran de servicio y se eliminan. La seguridad de la información se debería considerar en todas las etapas. Los nuevos desarrollos y cambios a los sistemas existentes presentan oportunidades para que las organizaciones actualicen y mejoren los controles de seguridad, considerando los incidentes reales y los riesgos de seguridad de la información actuales y proyectados.

0.6 Normas relacionadas

Si bien esta norma ofrece orientación sobre una amplia gama de controles de seguridad de la información que se aplican comúnmente en muchas organizaciones distintas, las normas restantes en la familia ISO/IEC 27000 brindan consejos o requisitos complementarios sobre el resto de los aspectos del proceso general de la administración de la seguridad de la información.

Consulte ISO/IEC 27000 para obtener una presentación general tanto de SGSI como de la familia de normas. ISO/IEC 27000 entrega un glosario, que define formalmente la mayoría de los términos que se utilizan en la familia de normas ISO/IEC 27000 y describe el alcance y los objetivos para cada miembro de la familia.

1 Alcance y campo de aplicación

Esta norma brinda orientación para las normas de seguridad de información organizacional y las prácticas de administración de seguridad de la información incluida la selección, la implementación, la administración y los controles considerando los entornos de riesgo de seguridad de la información de la organización.

Esta norma está diseñada para que la utilicen las organizaciones que tienen la intención de:

a) seleccionar controles dentro del proceso de implementación de un Sistema de Administración de Seguridad de la Información basado en ISO/IEC 27001;

b) implementar controles de seguridad de la información de aceptación común;

c) desarrollar sus propias pautas de administración de seguridad de la información.

2 Referencias normativas

El siguiente documento, en su totalidad o en parte, hace referencia a la normativa de este documento y es indispensable para su aplicación. Para las referencias con fechas, solo aplica la edición citada. Para las referencias sin fecha, se aplica la edición más reciente del documento al que se hace referencia (incluida cualquier modificación).

ISO/IEC 27000 *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

NOTA EXPLICATIVA NACIONAL

La equivalencia de la Norma Internacional señalada anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma internacional	Norma nacional	Grado de correspondencia
ISO/IEC 27000	No hay	-

3 Términos y definiciones

Para los propósitos de este documento, se aplican los términos y definiciones descritos en ISO/IEC 27000.

4 Estructura de esta norma

Esta norma contiene 14 cláusulas de control de seguridad que en conjunto contienen un total de 35 categorías de seguridad principales y 114 controles.

4.1 Cláusulas

Cada cláusula que define los controles de seguridad contiene una o más de las principales categorías de seguridad. El orden de las cláusulas en esta norma no implica su importancia. En función de las circunstancias, los controles de seguridad que provienen de cualquiera o todas las cláusulas podrían resultar importantes, por lo tanto, cada organización que aplica esta norma debería identificar los controles pertinentes, lo importante que son y su aplicación a los procesos comerciales individuales. Más aún, las listas de esta norma no se enumeran en orden de prioridad.

4.2 Categorías de control

Cada categoría de control de seguridad principal contiene:

a) un objetivo de control que indica lo que se logrará;

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

Las descripciones de control se estructuran de la siguiente forma:

Control

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

Orientación sobre la implementación

Proporciona información más detallada para apoyar la implementación del control y el cumplimiento del objetivo de control. Es posible que la orientación no sea completamente adecuada o suficiente en todas las situaciones y es posible que no cumpla con los requisitos de control específicos.

Otra información

Brinda más información que es posible que se deba considerar, por ejemplo, consideraciones legales y referencias a otras normas. Si no existe más información para proporcionar no se mostrará esta parte.

5 Políticas de seguridad de la información

5.1 Orientación de administración para la seguridad de la información

Objetivo: dar orientación y apoyo en la administración para la seguridad de la información de acuerdo con los requisitos comerciales y las leyes y normativas pertinentes.

5.1.1 Políticas para la seguridad de la información

Control

Se debería definir un conjunto de políticas para la seguridad de la información y la debería aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes.

Orientación sobre la implementación

En el nivel más alto, las organizaciones deberían definir una “política de seguridad de la información" que la aprueba la dirección y que establece el enfoque de la organización para administrar sus objetivos de seguridad de la información.

Las políticas de seguridad de la información deberían abordar los requisitos creados por:

a) estrategia comercial;

b) normativas, legislación y contratos;

c) el entorno de amenazas a la seguridad actual y proyectada.

La política de seguridad de la información debería tener enunciados respecto a lo siguiente:

a) definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;

b) asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;

c) procesos para manejar desviaciones y excepciones.

A un nivel inferior, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, que estipula la implementación de controles de seguridad de la información y que típicamente se estructura para abordar las necesidades de ciertos grupos objetivo dentro de una organización para abarcar ciertos temas.

Algunos ejemplos de dichos temas de políticas incluyen:

a) control de accesos (ver cláusula 9);

b) clasificación de la información (y manejo) (ver 8.2);

c) seguridad física y ambiental (ver cláusula 11);

d) temas orientados al usuario final como:

    1) uso aceptable de activos (ver 8.1.3);

    2) escritorio despejado y pantalla despejada (ver 11.2.9);

    3) transferencia de información (ver 13.2.1);

    4) dispositivos móviles y teletrabajo (ver 6.2);

    5) restricciones sobre las instalaciones y el uso de software (ver 12.6.2);

e) respaldo (ver 12.3);

f) transferencia de información (ver 13.2);

g) protección contra malware (ver 12.2);

h) administración de vulnerabilidades técnicas (ver 12.6.1);

i) controles criptográficos (ver cláusula 10);

j) seguridad en las comunicaciones (ver cláusula 13);

k) privacidad y protección de información personal identificable (ver 18.1.4);

l) relaciones con los proveedores (ver cláusula 15).

Estas políticas se deberían comunicar a los empleados y a las partes externas pertinentes de una forma pertinente, accesible y comprensible para el lector deseado, es decir, en el contexto de un *programa de concientización, educación y capacitación sobre la seguridad de la información* (ver 7.2.2).

Otra información

La necesidad de contar con políticas internas para la seguridad de la información varía entre las organizaciones. Las políticas internas son especialmente útiles en organizaciones de mayor tamaño y complejidad, donde aquellos que definen y aprueban los niveles ampliados de control se segregan de los que implementan los controles o en situaciones donde una política se aplica a varias personas o funciones distintas de la organización. Las políticas para la seguridad de la información se pueden emitir en un documento de *política de seguridad de la información* único o como un conjunto de documentos individuales pero relacionados.

Si se distribuye cualquier parte de las políticas de seguridad de la información fuera de la organización, se debería tener cuidado de no divulgar información confidencial.

Algunas organizaciones utilizan otros términos para estos documentos de políticas como “Normas”, “Directivas” o “Reglas”.

5.1.2 Revisión de las políticas para la seguridad de la información

Control

Las políticas para la seguridad de la información se deberían planificar y revisar en intervalos o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad continua.

Orientación sobre la implementación

Cada política debería tener un titular que tenga responsabilidad administrativa aprobada para el desarrollo, la revisión y la evaluación de las políticas. La revisión debería incluir la evaluación de oportunidades de mejora en las políticas de la organización y un enfoque para administrar la seguridad de la información en respuesta a los cambios en el entorno organizacional, las circunstancias comerciales, las condiciones legales o el entorno técnico.

La revisión de las políticas de la seguridad de la información debería considerar los resultados de las revisiones administrativas.

Se debería obtener la aprobación de la dirección para una política revisada.

6 Organización de la seguridad de la información

6.1 Organización interna

Objetivo: establecer un marco de administración para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

6.1.1 Revisiones de los roles y responsabilidades de la seguridad en la información

Control

Se deberían definir y asignar todas las responsabilidades de seguridad de la información.

Orientación sobre la implementación

La asignación de las responsabilidades de seguridad de la información se debería hacer de acuerdo con las políticas de seguridad de la información (ver 5.1.1). Se deberían identificar las responsabilidades para la protección de activos individuales y para realizar procesos de seguridad de la información. Se deberían definir las responsabilidades para las actividades de administración de riesgos de seguridad de la información y en particular para la aceptación de riesgos residuales. Estas responsabilidades se deberían complementar, donde sea necesario, con orientación más detallada para los sitios específicos y las instalaciones de procesamiento de información. Se deberían definir las responsabilidades para la protección de activos para realizar procesos de seguridad de la información.

Las personas asignadas con responsabilidades de seguridad de la información pueden delegar las tareas de seguridad a otros. Sin embargo, siguen siendo responsables y deberían determinar que cualquier tarea delegada se haya realizado correctamente.

Se deberían indicar las áreas por las que las personas son responsables. En particular, debería ocurrir lo siguiente:

a) se deberían definir e identificar los actives y los procesos de seguridad de la información;

b) se debería asignar a la entidad responsable de cada activo o proceso de seguridad de la información y se deberían documentar los detalles de la responsabilidad (ver 8.1.2);

c) se deberían definir y documentar los niveles de autorización;

d) para poder cumplir con las responsabilidades en el área de seguridad de la información, las personas asignadas deberían ser competentes en el área y deberían contar con oportunidades para mantenerse al día en los desarrollos;

e) se debería identificar y documentar la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores.

Otra información

Muchas organizaciones asignan a un gerente de seguridad de la información para tomar la responsabilidad general del desarrollo y la implementación de la seguridad de la información y para apoyar la identificación de controles.

Sin embargo, la responsabilidad para asignar recursos e implementar los controles a menudo estará a cargo de los gerentes individuales. Una práctica común es asignar a un titular para cada activo quien luego se hace responsable de su protección diaria.

6.1.2 Segregación de deberes

Control

Se deberían segregar los deberes y áreas de responsabilidad en conflicto para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de la organización.

Orientación sobre la implementación

Se debería tener cuidado para que ninguna persona pueda acceder, modificar ni utilizar activos sin autorización o detección. El inicio de un evento se debería separar de su autorización. Se debería considerar la posibilidad de colusión en el diseño de controles.

Las organizaciones pequeñas pueden encontrar la segregación de labores como difícil de lograr, pero el principio se debería aplicar en la mayor medida posible. Cuando sean difíciles de segregar, se deberían considerar otros controles como el monitoreo de actividades, seguimientos de auditoría y supervisión de la dirección.

Otra información

La segregación de deberes es un método para reducir el riesgo de uso accidental o indebido deliberado de los activos de una organización.

6.1.3 Contacto con las autoridades

Control

Se deberían mantener los contactos con las autoridades pertinentes correspondientes.

Orientación sobre la implementación

Las organizaciones deberían tener procedimientos en vigencia que especifiquen cuándo y a qué autoridades (es decir, de cumplimiento de la ley, entidades regulatorias, autoridades de supervisión) se debería contactar y cómo se deberían informar los incidentes de seguridad de la información identificados de manera oportuna (es decir, si se sospecha del incumplimiento de las leyes).

Otra información

Es posible que las organizaciones bajo ataques de internet deban tomar medidas contra el origen del ataque. Mantener esos contactos puede ser un requisito para apoyar a la administración de incidentes de la seguridad de la información, (ver cláusula 16) o el proceso de continuidad comercial y planificación de contingencia (ver cláusula 17). Los contactos con las entidades normativas también resultan útiles para anticiparse y prepararse para los cambios futuros en las leyes o normativas, que debería implementar la organización. Los contactos con otras autoridades incluyen a los proveedores de servicios básicos, de servicios de emergencia, electricidad, salud y seguridad, es decir, departamentos de bomberos (en conexión con la continuidad comercial), proveedores de telecomunicaciones (en conexión con el enrutamiento de línea y disponibilidad) y proveedores de agua (en conexión con las instalaciones de enfriamiento para el equipo).

6.1.4 Contacto con grupos de interés especiales

Control

Se deberían mantener los contactos adecuados con grupos de interés especiales u otros foros de seguridad de especialistas y asociaciones profesionales.

Orientación sobre la implementación

La membresía en grupos o foros de interés especiales se debería considerar como un medio para:

a) mejorar el conocimiento sobre las buenas prácticas y permanecer al tanto de la información de seguridad pertinente;

b) asegurarse de que la comprensión del entorno de seguridad de la información sea actual y completo;

c) recibir alertas tempranas de alertas, avisos y parches relacionados con los ataques y vulnerabilidades;

d) obtener acceso a información de especialistas sobre consejos de seguridad;

e) compartir e intercambiar información sobre las nuevas tecnologías, productos, amenazas y vulnerabilidades

f) proporcionar puntos de enlace adecuados al tratar con incidentes de seguridad de la información (ver cláusula 16).

Otra información

Se pueden establecer acuerdos para compartir información a modo de mejorar la cooperación y la coordinación de los problemas de seguridad. Dichos acuerdos deberían identificar los requisitos para la protección de información confidencial.

6.1.5 Seguridad de la información en la administración de proyectos

Control

Se debería abordar la seguridad de la información en la administración de proyectos, sin importar el tipo de proyecto.

Orientación sobre la implementación

Se debería integrar la seguridad de la información en los métodos de administración de proyectos de la organización para asegurarse de que se identifican y abordan los riesgos de seguridad de la información como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, sin importar su carácter, es decir, un proyecto para un proceso comercial central, TI, administración de instalaciones y otros procesos de apoyo. Los métodos de administración de proyectos en uso deberían requerir que:

a) se incluyan los objetivos de seguridad de la información en los objetivos del proyecto.

b) se realice una evaluación de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios;

c) la seguridad de la información sea parte de todas las fases de la metodología aplicada del proyecto.

Se deberían abordar y revisar las implicaciones de seguridad de manera regular en todos los proyectos. Se deberían definir y asignar las responsabilidades para la seguridad de la información a los roles especificados definidos en los métodos de administración del proyecto.

6.2 Dispositivos móviles y teletrabajo

Objetivo: garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política de dispositivos móviles

Control

Se debería adoptar una política y medidas de seguridad de apoyo para administrar los riesgos que se presentan con el uso de dispositivos móviles.

Orientación sobre la implementación

Al utilizar dispositivos móviles, se debería tener cuidado de asegurar que la información comercial no se vea comprometida. La política de dispositivos móviles debería considerar los riesgos de trabajar con dispositivos móviles en entornos sin protección.

La política de dispositivos móviles debería considerar:

a) registro de dispositivos móviles;

b) requisitos para la protección física;

c) restricción de la instalación de software;

d) requisitos para las versiones de software de dispositivos móviles para la aplicación de parches;

e) restricción en la conexión a servicios de información;

f) controles de acceso;

g) técnicas criptográficas;

h) protección contra malware;

i) deshabilitación, borrado o bloqueo remoto;

j) respaldos;

k) uso de servicios web y aplicaciones web.

Se debería ser cuidadoso al utilizar dispositivos móviles en lugares públicos, salas de reuniones y otras áreas sin protección. Se debería contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos, es decir, mediante el uso de técnicas criptográficas (ver cláusula 10) y mediante la obligación del uso de información de autenticación secreta (ver 9.2.4).

Los dispositivos móviles también se deberían proteger físicamente contra el robo, especialmente cuando se dejan, por ejemplo, en automóviles u otros medios de transporte, en habitaciones de hotel, centros de conferencia y lugares de reunión. Se debería establecer un procedimiento específico que considere los requisitos legales, de seguros y otros de seguridad de la organización para casos de robo o pérdida de dispositivos móviles. Los dispositivos que contengan información comercial importante, sensible o crítica no se deberían dejar sin supervisión y, donde sea posible, se deberían guardar con llave o se deberían utilizar bloqueos especiales para proteger a los dispositivos.

Se deberían organizar capacitaciones para el personal que utiliza dispositivos móviles y concientizarlos sobre los riesgos adicionales que genera esta forma de trabajo y los controles que se deberían implementar.

Donde la política de dispositivos móviles permita el uso de dispositivos móviles de propiedad privada, la política y las medidas de seguridad relacionadas también deberían considerar:

a) separación del uso privado y comercial de los dispositivos, incluido el uso de software para apoyar dicha separación y proteger los datos comerciales en un dispositivo privado;

b) proporcionar acceso a la información comercial solo después de que los usuarios hayan firmado un acuerdo de usuario final que reconozca sus deberes (protección física, actualización de software, etc.), renunciando a la propiedad de los datos comerciales, permitiendo el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo o cuando ya no esté autorizado a utilizar el servicio. Esta política debería considerar la legislación de privacidad.

Otra información

Las conexiones inalámbricas de dispositivos móviles son similares a otros tipos de conexión de redes, pero tienen diferencias importantes que se deberían considerar al identificar los controles. Las diferencias típicas son:

a) algunos protocolos de seguridad inalámbricas son inmaduros y tienen debilidades conocidas;

b) es posible que la información almacenada en dispositivos no se respalde en los dispositivos móviles debido a un ancho de banda limitado o debido a que los dispositivos móviles pueden no estar siempre conectados cuando se han programado los respaldos.

Los dispositivos móviles generalmente comparten funciones comunes, es decir, el funcionamiento en redes, el acceso a internet, correo electrónico y el manejo de archivos con dispositivos de uso fijo. Los controles de seguridad de la información para los dispositivos móviles generalmente constan de aquellos adoptados en dispositivos de uso fijo y aquellos que abordan las amenazas que surgen de su uso fuera de las dependencias de la organización.

6.2.2 Teletrabajo

Control

Se debería implementar una política y medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de teletrabajo.

Orientación sobre la implementación

Las organizaciones que permiten las actividades de teletrabajo deberían emitir una política que define las condiciones y las restricciones del uso del teletrabajo. Se deberían considerar los siguientes asuntos donde se considere aplicable y lo permita la ley:

a) la seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;

b) el entorno de teletrabajo físico propuesto;

c) los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que se traspasará por el enlace de comunicaciones y la sensibilidad del sistema interno;

d) la provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;

e) la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;

f) el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;

g) las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;

h) acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;

i) acuerdos de licenciamiento de software que pueden hacer que las organizaciones se hagan responsables del software de cliente en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;

j) requisitos de protección de malware firewall (cortafuegos).

Las pautas y disposiciones que se deberían consideran deberían incluir:

a) la provisión de equipos idóneos y muebles de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;

b) una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;

c) la provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;

d) seguridad física;

e) normas y orientación sobre el acceso a familiares y visitas a los equipos y a la información;

f) la provisión de soporte y mantenimiento de hardware y software;

g) la provisión de seguros;

h) los procedimientos para el respaldo y la continuidad en el negocio;

i) auditoría y monitoreo de seguridad;

j) revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.

Otra información

El teletrabajo se refiere a todas las formas de trabajo fuera de la oficina, incluidos los ambientes de trabajo no tradicionales, como los que se conocen como entornos de “teleconmutación”, “lugar de trabajo flexible”, “trabajo remoto” y “trabajo virtual”.

7 Seguridad de recursos humanos

7.1 Antes del empleo

Objetivo: garantizar que los empleados y contratistas comprendan sus responsabilidades y que sean adecuados para los roles en los que se les ha considerado.

7.1.1 Selección

Control

La verificación de antecedentes de todos los candidatos para el empleo se debería realizar de acuerdo a las leyes, normativas y ética pertinentes y debería ser proporcional a los requisitos del negocio, la clasificación de la información a la que se accederá y los riesgos percibidos.

Orientación sobre la implementación

La verificación debería considerar toda la privacidad y la protección pertinente de la información identificable personalmente y la legislación basada en el empleo y, donde se permita, debería incluir lo siguiente:

a) disponibilidad de referencias de carácter satisfactorias, es decir una comercial y una personal;

b) una verificación (de integridad y precisión) del currículum vitae del postulante;

c) confirmación de las calificaciones académicas y profesionales que se indican;

d) verificación de identidad independiente (pasaporte o un documento similar);

e) verificación en mayor detalle, como una revisión al historial de crédito o los antecedentes penales.

Cuando se contrata a una persona para un rol de seguridad de la información específico, las organizaciones se deberían asegurar de que el candidato:

a) cuente con las competencias necesarias para desempeñar el rol de seguridad;

b) pueda ser confiable para asumir el rol, en especial si éste es fundamental para la organización.

Donde un trabajo, ya sea de empleo inicial o por ascenso, requiera que la persona tenga acceso a las instalaciones de procesamiento de información y, en particular, si se maneja información confidencial, es decir, información financiera o altamente confidencial, la organización también debería considerar más verificaciones y en mayor detalle.

Los procedimientos deberían definir los criterios y limitaciones para las revisiones de verificación, es decir, quién es idóneo para seleccionar a las personas y cómo, cuándo y por qué se realizan las revisiones de verificación.

También se debería garantizar un proceso de selección para los contratistas. En estos casos, donde el acuerdo entre la organización y el contratista debería especificar las responsabilidades para realizar la selección y los procedimientos de notificación que se deberían seguir si la selección no ha finalizado o si los resultados dan motivo para dudas o inquietudes.

La información de todos los candidatos que se están considerando para puestos dentro de la organización se deberían recopilar y manejar de acuerdo a cualquier legislación correspondiente existente en la jurisdicción pertinente. En función de la legislación pertinente, se debería informar a los candidatos de antemano sobre las actividades de selección.

7.1.2 Términos y condiciones de empleo

Control

Los acuerdos contractuales con los empleados y contratistas deberían indicar sus responsabilidades y las de la organización para la seguridad de la información.

Orientación sobre la implementación

Las obligaciones contractuales para los empleados o los contratistas deberían reflejar las políticas de la organización para la seguridad de la información además de aclarar e indicar:

a) que todos los empleados y contratistas a los que se les otorga acceso a información confidencial deberían firmar un acuerdo de confidencialidad y no divulgación antes de darles acceso a las instalaciones de procesamiento de información (ver 13.2.4);

b) las responsabilidades legales y derechos del empleado o del contratista, es decir, en cuanto a las leyes de derecho de autor o de la legislación de protección de datos (ver 18.1.2 y 18.1.4);

c) responsabilidades para la clasificación de la información y la administración de activos organizacionales asociados a la información, las instalaciones de procesamiento de información y los servicios de información que maneja el empleado o contratista (ver cláusula 8);

d) responsabilidades del empleado o contratista para manejar la información recibida de otras empresas o partes externas;

e) medidas que se deberían tomar si el empleado o contratista no cumple con los requisitos de seguridad de la organización (ver 7.2.3).

Los roles y responsabilidades de seguridad de la información se deberían comunicar a los postulantes al trabajo durante el proceso previo al empleo.

La organización se debería asegurar de que todos los empleados y contratistas estén de acuerdo con los términos y condiciones en cuanto a la seguridad de la información conforme a la naturaleza y al alcance del acceso que tendrán a los activos de la organización asociados a los sistemas y servicios de información.

Donde corresponda, las responsabilidades incluidas en los términos y condiciones de empleo deberían continuar por un período definido después del término del empleo (ver 7.3).

Otra información

Se puede utilizar un código de conducta para indicar las responsabilidades en cuanto a la seguridad de la información del empleado o contratista respecto de la confidencialidad, la protección de datos, la ética, el uso adecuado del equipo y las instalaciones de la organización, así como las prácticas honorables que espera la organización. Se puede solicitar a una parte externa asociada con un contratista a iniciar disposiciones contractuales a nombre de la persona contratada.

7.2 Durante el empleo

Objetivo: asegurarse de que los empleados y contratistas están en conocimiento de y que cumplen con sus responsabilidades de seguridad de la información.

7.2.1 Responsabilidades de la dirección

Control

La dirección debería exigir a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.

Orientación sobre la implementación

Las responsabilidades de la dirección deberían incluir asegurarse de que los empleados y los contratistas:

a) cuenten con instrucciones preliminares sobre sus roles y responsabilidades de seguridad de la información antes de que se les otorgue acceso a la información confidencial o a los sistemas de información;

b) se les entreguen pautas para indicar las expectativas de seguridad de la información en su rol dentro de la organización;

c) se les motive para cumplir con las políticas de seguridad de la información de la organización;

d) logren un nivel de concientización sobre la seguridad de la información conforme a sus roles y responsabilidades dentro de la organización (ver 7.2.2);

e) cumplan con los términos y condiciones de empleo, que incluye la política de seguridad de información de la organización y los métodos de trabajo correspondientes;

f) continúen teniendo las habilidades y calificaciones adecuadas y que se capaciten de manera regular;

g) se les proporcione un canal de denuncias anónimas para denunciar transgresiones a las políticas y procedimientos de seguridad de la información (“poner de manifiesto”).

La dirección debería demostrar su apoyo a las políticas, los procedimientos y los controles de seguridad de la información y actuar como un modelo a seguir.

Otra información

Si a los empleados o contratistas no se les dan a conocer sus responsabilidades de seguridad de la información, pueden provocar daños considerables a la organización. El personal motivado tiene mayores probabilidades de ser más confiable y provocar menos incidentes de seguridad de la información.

Una administración deficiente puede hacer que el personal se sienta subvalorado, lo que genera un impacto negativo en la seguridad de la información de la organización. Por ejemplo, una administración deficiente puede llevar al olvido de la seguridad de la información o al posible uso indebido de los activos de la organización.

7.2.2 Concientización, educación y capacitación sobre la seguridad de la información

Control

Todos los empleados de la organización y, donde sea pertinente, los contratistas deberían recibir educación y capacitación de concientización adecuada y actualizaciones regulares sobre las políticas y procedimientos organizacionales, según sea pertinente para su función laboral.

Orientación sobre la implementación

Un programa de concientización sobre seguridad de la información debería apuntar a hacer que los empleados y, donde resulte pertinente, los contratistas conozcan sus responsabilidades en cuanto a la seguridad de la información y los medios a través de los que se descargan esas responsabilidades.

Un programa de concientización de seguridad de la información se debería establecer de acuerdo con las políticas y procedimientos pertinentes de seguridad de la información de la organización, considerando la información de la organización que se va a proteger y los controles que se han implementado para proteger la información. El programa de concientización debería incluir varias actividades de concientización como campañas (por ejemplo, un “día de la seguridad de la información”) y la entrega de panfletos o boletines informativos.

El programa de concientización se debería planificar considerando los roles de los empleados en la organización y, donde corresponda, la expectativa que tiene la organización sobre la concientización de los contratistas. Las actividades del programa de concientización se deberían programar con el tiempo, de preferencia de manera regular, para que las actividades se repitan y abarquen a los nuevos empleados y contratistas. El programa de concientización también se debería actualizar de manera regular para que esté de acuerdo con las políticas y procedimientos de la organización y se debería basar en las lecciones aprendidas de los incidentes de seguridad de la información.

Se debería realizar una capacitación de concientización según lo requiera el programa de concientización de seguridad de la información de la organización. La capacitación de concientización se puede realizar a través de distintos medios incluida la capacitación en el aula, a distancia, en línea, autónoma y otros.

La educación y la capacitación de seguridad de la información también debería abarcar aspectos generales como:

a) indicar el compromiso de la dirección con la seguridad de la información en toda la organización;

b) la necesidad de conocer y cumplir con las normas y obligaciones de seguridad de la información pertinentes, según se define en las políticas, normas, leyes, normativas, contratos y acuerdos;

c) responsabilidad personal por las acciones e inoperancias propias y las responsabilidades generales hacia el aseguramiento y protección de la información que pertenece a la organización y a las partes externas.

d) procedimientos básicos de seguridad de la información (como la denuncia de incidentes de seguridad de la información) y controles de la línea de base (como seguridad de contraseñas, controles de malware y despeje de escritorios);

e) Puntos de contacto y recursos para la información adicional y asesoría sobre los asuntos de seguridad de la información, incluida una mayor información sobre la educación y los materiales de capacitación para la seguridad de la información.

La educación y la capacitación sobre la seguridad de la información se debería realizar de manera periódica. La educación y la capacitación inicial se aplica a quienes se les traslada a nuevos cargos o roles con requisitos de seguridad de la información sustancialmente diferentes, no solo para quienes comienzan sus labores y, se debería realizar antes de que el rol se active.

La organización debería desarrollar el programa de educación y capacitación para poder realizar la educación y la capacitación de manera eficaz. El programa se debería establecer de acuerdo con las políticas y procedimientos pertinentes de seguridad de la información de la organización, considerando la información de la organización que se va a proteger y los controles que se han implementado para proteger la información. El programa debería considerar las distintas formas de educación y capacitación, es decir, charlas o estudio autónomo.

Otra información

Al comprometerse en un programa de concientización, es importante no solo centrarse en el “qué” y en el “cómo”, sino que también en el “por qué”. Es importante que los empleados entiendan el objetivo de la seguridad de la información y el posible impacto, ya sea positivo y negativo, en la organización y en su propio comportamiento.

La concientización, la educación y la capacitación pueden ser parte de o realizarse en colaboración con otras actividades de capacitación, por ejemplo, un programa general de TI o de seguridad general. Las actividades de concientización, la educación y la capacitación deberían ser adecuadas y pertinentes para los roles, las responsabilidades y las habilidades de las personas.

Se puede realizar una evaluación del conocimiento de los empleados al final de un curso de concientización, educación y capacitación para probar la transferencia de conocimiento.

7.2.3 Proceso disciplinario

Control

Debería haber un proceso disciplinario formal y comunicado en vigencia para tomar medidas contra los empleados que se han involucrado en una transgresión a la seguridad de la información.

Orientación sobre la implementación

El proceso disciplinario no se debería iniciar antes de verificar que ha ocurrido una transgresión a la seguridad de la información (ver 16.1.7).

El proceso disciplinario formal debería garantizar un trato justo y correcto para los empleados sospechosos de cometer violaciones a la seguridad de la información. El proceso disciplinario formal debería proporcionar una respuesta gradual que considere factores como la naturaleza y la gravedad de la transgresión y su impacto en el negocio, ya sea o no el primer agravio o una repetición, ya sea o no que el transgresor haya sido capacitado adecuadamente, la legislación pertinente, los contratos comerciales u otros factores según sea necesario.

El proceso disciplinario también se debería utilizar como elemento disuasivo para evitar que los empleados transgredan las políticas y procedimientos de seguridad de la información de la organización y otras violaciones de la seguridad de la información. Las transgresiones deliberadas pueden requerir acciones inmediatas.

Otra información

El proceso disciplinario también puede convertirse en una motivación o en un incentivo si se definen sanciones positivas para el comportamiento sobresaliente en cuanto a la seguridad de la información.

7.3 Despido y cambio de empleo

Objetivo: proteger los intereses de la organización como parte del proceso de cambiar de o finalizar el empleo.

7.3.1 Despido o cambio de responsabilidades en el empleo

Control

Las responsabilidades y deberes de la seguridad de la información que siguen vigentes después de un despido o cambio de empleo se deberían definir, comunicar al empleado o contratista y hacer cumplir.

Orientación sobre la implementación

La comunicación del cese de responsabilidades debería incluir requisitos de seguridad de la información y responsabilidades legales constantes y, donde corresponda, las responsabilidades incluidas dentro de cualquier acuerdo de confidencialidad (ver 13.2.4) y los términos y condiciones de empleo (ver 7.1.2) que continúan por un período definido después del fin del empleo del empleado o del contratista.

Las responsabilidades y deberes que aún siguen siendo válidos después del fin del empleo deberían incluirse en los términos y condiciones de empleo del empleado o contratista (ver 7.1.2).

Los cambios en las responsabilidades o en el empleo se deberían manejar como en la finalización de la responsabilidad actual o el empleo en combinación con la iniciación de la nueva responsabilidad o empleo.

Otra información

La función de recursos humanos es generalmente ser responsable del proceso de despido general y trabaja con el gerente que supervisa a la persona que abandona la organización para administrar los aspectos de seguridad de la información de los procedimientos pertinentes. En el caso de un contratista quien presta servicios a través de terceros, este proceso de despido lo realizará la parte externa de acuerdo con el contrato entre la organización y la parte externa.

Puede ser necesario informar a los empleados, a los clientes o a los contratistas sobre los cambios de personal y a las disposiciones operativas.

8 Administración de activos

8.1 Responsabilidad por los activos

Objetivo: identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.

8.1.1 Inventario de activos

Control

Se deberían identificar los activos asociados a la información y las instalaciones de procesamiento de información y se debería elaborar y mantener un inventario de estos activos.

Orientación sobre la implementación

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.

Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.

El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad (ver 8.1.2) y clasificación. (Ver 8.2).

Otra información

Los inventarios de activos ayudan a garantizar que se implementa una protección eficaz y también pueden ser necesarios para otros propósitos como la salud y seguridad y por motivos de seguros o financieros (administración de activos).

La norma ISO/IEC 27005 brinda ejemplos de los activos que la organización puede considerar necesarios al identificar activos. El proceso de compilación de un inventario de activos es un prerrequisito importante de la administración de activos (ver ISO/IEC 27000 e ISO/IEC 27005).

8.1.2 Propiedad de los activos

Control

Los activos mantenidos en el inventario deberían ser propietarios.

Orientación sobre la implementación

Las personas, así como también otras entidades que tienen responsabilidad de la dirección aprobada para el ciclo de vida de los activos califican para ser asignados como propietarios de activos.

Generalmente se implementa un proceso para asegurar la asignación oportuna de la propiedad de los activos. Se debería asignar la propiedad de los activos cuando éstos se crean o cuando se transfieren a la organización. El propietario del activo debería responsable de la administración correcta de un activo durante todo su ciclo de vida.

El propietario del activo debería:

a) garantizar que se haga un inventario de todos los activos;

b) asegurarse de que los activos se clasifiquen y protejan adecuadamente;

c) definir y revisar periódicamente las restricciones de acceso y clasificaciones para los activos importantes, considerando las políticas de control de acceso pertinentes;

d) asegurarse de un manejo adecuado cuando se elimine o destruya un activo.

Otra información

El propietario identificado puede ser una persona o una entidad que cuente con responsabilidad de la dirección aprobada para controlar todo el ciclo de vida de un activo. El propietario identificado no necesariamente tiene derechos de propiedad del activo.

Se pueden delegar las tareas rutinarias, es decir a un custodio que resguarde los activos diariamente, pero la responsabilidad sigue siendo del propietario.

En sistemas de información complejos, puede resultar útil asignar grupos de activos que actúen en conjunto para brindar un servicio en particular. En este caso el propietario de este servicio es responsable de la entrega del servicio, incluida la operación de sus activos.

8.1.3 Uso aceptable de activos

Control

Se deberían identificar, documentar e implementar las reglas para el uso aceptable de la información de los activos asociados a la información y a las instalaciones de procesamiento de información.

Orientación sobre la implementación

Los empleados y los usuarios externos que utilizan o tienen acceso a los activos de la organización deberían estar al tanto de los requisitos de seguridad de la información de los activos de la organización asociados a la información y a las instalaciones y recursos de procesamiento de información. Deberían ser responsables del uso de cualquier recurso de procesamiento de información y cualquier tipo de uso como tal se debería realizar bajo su responsabilidad.

8.1.4 Devolución de activos

Control

Todos los empleados y usuarios externos deberían devolver todos los activos organizacionales en su poder al finalizar su empleo, contrato o acuerdo.

Orientación sobre la implementación

El proceso de finalización de empleo se debería formalizar para incluir la devolución de todos los activos físicos y electrónicos previamente entregados de propiedad de o encomendados a la organización.

En los casos donde un empleado o un externo compre el equipo de la organización o utilice sus propios equipos personales, se deberían seguir los procedimientos para garantizar que la información pertinente se transfiera a la organización y que se elimine de manera segura del equipo (ver 11.2.7).

En los casos donde el empleado o el usuario externo cuenta con conocimiento importante para las operaciones continuas, dicha información se debería documentar y transferir a la organización.

Durante el período de aviso de despido, la organización debería controlar las copias no autorizadas de la información pertinente (es decir, propiedad intelectual) de los empleados y contratistas despedidos.

8.2 Clasificación de la información

Objetivo: asegurar que la información reciba el nivel de protección adecuado de acuerdo con su importancia para la organización.

8.2.1 Clasificación de información

Control

La información se debería clasificar en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación no autorizada.

Orientación sobre la implementación

Las clasificaciones y los controles de protección asociados de la información deberían considerar las necesidades que tiene el negocio de compartir o restringir información, así como también los requisitos legales. Los activos que no sean información también se pueden clasificar de acuerdo con la clasificación de información que se almacena en, procesa por o de otro modo, maneja o protege el activo.

Los propietarios de los activos de información deberían ser responsables de su clasificación.

El esquema de clasificación debería incluir las convenciones para la clasificación y los criterios para la revisión de la clasificación con el tiempo. El nivel de protección del esquema se debería evaluar mediante el análisis de la confidencialidad, la integridad y la disponibilidad de cualquier otro requisito para la información considerada. El esquema debería estar alineado con la política de control de acceso (ver 9.1.1).

A cada nivel se le debería asignar un nombre que tenga sentido en el contexto del esquema de clasificación de la aplicación. El esquema se debería considerar en toda la organización para que todos clasifiquen la información y los activos relacionados de la misma forma, cuenten con un entendimiento común de los requisitos de protección y apliquen la protección adecuada.

La clasificación se debería incluir en los procesos de la organización y debería ser coherente y consistente en toda la organización. Los resultados de la clasificación deberían indicar el valor de los activos en función de su sensibilidad y criticidad para la organización, es decir, en términos de confidencialidad, integridad y disponibilidad. Los resultados de la clasificación se deberían actualizar de acuerdo con los cambios en su valor, sensibilidad y criticidad a través de su ciclo de vida.

Otra información

La clasificación le entrega a las personas que se encargan de la información una indicación concisa sobre cómo manejarla y protegerla. La creación de grupos de información con necesidades de protección similares y la especificación de los procedimientos de seguridad de la información que se aplican a toda la información en cada grupo facilita este proceso. Este enfoque reduce la necesidad de una evaluación de riesgo caso a caso y el diseño personalizado de controles.

La información puede dejar de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos se deberían considerar, pues la sobre clasificación puede llevar a la implementación de controles innecesarios, lo que generará gastos adicionales o, por el contrario, la falta de clasificación puede poner en peligro el logro de los objetivos comerciales.

Un ejemplo de un esquema de clasificación de confidencialidad de la información se puede basar en cuatro niveles de la siguiente manera:

a) la divulgación no hace daño;

b) la divulgación provoca una vergüenza menor o una inconveniencia operacional menor;

c) la divulgación tiene un impacto significativo a corto plazo en las operaciones o en los objetivos tácticos;

d) la divulgación tiene un impacto grave en los objetivos estratégicos a largo plazo o pone en riesgo la sobrevivencia de la organización.

8.2.2 Etiquetado de información

Control

Se debería desarrollar e implementar un conjunto de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización.

Orientación sobre la implementación

Los procedimientos para el etiquetado de la información deberían cubrir la información y sus activos relacionados en formatos físicos o electrónicos. El etiquetado debería reflejar el esquema de clasificación establecido en 8.2.1. Las etiquetas se deberían poder reconocer fácilmente. Los procedimientos deberían brindar orientación sobre dónde y cómo se adhieren las etiquetas considerando cómo se accede a la información o cómo se manejan los activos en función de los tipos de medios. Los procedimientos pueden definir los casos donde se omite el etiquetado, es decir, etiquetando la información no confidencial para reducir las cargas de trabajo. Los empleados y contratistas deberían estar al tanto de los procedimientos de etiquetado.

Las salidas de los sistemas que contienen información clasificada como sensible o crítica deberían tener una etiqueta de clasificación adecuada.

Otra información

El etiquetado de información clasificada es un requisito clave para los acuerdos para compartir información. Las etiquetas físicas y los metadatos son una forma común de etiquetado.

El etiquetado de información y sus activos relacionados pueden tener efectos negativos a veces. Los activos clasificados son más fáciles de identificar y, en consecuencia, de sufrir robos de personas internas o de atacantes externos.

8.2.3 Manejo de activos

Control

Se deberían desarrollar e implementar procesos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.

Orientación sobre la implementación

Se deberían crear procesos para el manejo, procesamiento, almacenamiento y comunicación de la información conforme a su clasificación (ver 8.2.1).

Se deberían considerar los siguientes elementos:

a) restricciones de acceso que apoyen los requisitos de protección para cada nivel de clasificación;

b) mantenimiento de un registro formal de los receptores de activos autorizados;

c) protección de copias temporales o permanentes de información a un nivel coherente con la protección de la información original;

d) almacenamiento de los activos de TI de acuerdo con las especificaciones del fabricante;

e) marcado claro de todas las copias de medios para la atención del receptor autorizado.

El esquema de clasificación que se utiliza dentro de la organización puede no ser equivalente a los esquemas que utilizan otras organizaciones, incluso si los nombres de los niveles son similares; además, la información que se mueve entre las organizaciones puede variar en su clasificación en función de su contexto en cada organización, incluso si sus esquemas de clasificación son idénticos.

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

8.3 Manejo de medios

Objetivo: evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios.

8.3.1 Administración de medios extraíbles

Control

Se deberían implementar procedimientos para la administración de medios extraíbles de acuerdo con el esquema de clasificación adoptado por la organización.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para la administración de medios extraíbles:

a) si ya no es necesario, el contenido de cualquier medio reutilizable que será retirado de la organización se debería hacer irrecuperable.

b) donde sea necesario y práctico, se debería requerir una autorización para los medios retirados de la organización y se debería mantener un registro de tales retiros para poder mantener un seguimiento de auditoría.

c) todos los medios se deberían almacenar en un entorno seguro y protegido, de acuerdo con las especificaciones del fabricante.

d) si la confidencialidad o la integridad de los datos son consideraciones importantes, se deberían utilizar técnicas criptográficas para proteger los datos de los medios extraíbles;

e) para mitigar el riesgo de que los medios se degraden mientras aún se necesitan los datos almacenados, los datos se deberían transferir a medios nuevos antes de que se vuelvan ilegibles;

f) se deberían almacenar varias copias de datos valiosos en medios separados para reducir aún más el riesgo accidental de daños o pérdidas de datos

g) se debería considerar un registro de medios extraíbles para limitar la oportunidad de pérdidas de datos.

h) las unidades de medios extraíbles solo se deberían habilitar si existe una razón comercial para ello;

i) donde exista la necesidad de utilizar medios extraíbles, se debería monitorear la transferencia de información a dichos medios.

Se deberían documentar los procedimientos y los niveles de autorización.

8.3.2 Eliminación de medios

Control

Los medios se deberían eliminar de manera segura cuando ya no se necesitan, a través de procedimientos formales.

Orientación sobre la implementación

Se deberían establecer procedimientos formales para la eliminación segura de los medios, a fin de minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Los procedimientos para la eliminación segura de medios que contienen información confidencial deberían ser proporcionales a la sensibilidad de esa información. Se deberían considerar los siguientes elementos:

a) los medios que contienen información confidencial se deberían almacenar y eliminar de manera segura, es decir, mediante la incineración, o la destrucción o bien a través del borrado de datos para el uso por parte de otra aplicación dentro de la organización;

b) deberían existir procedimientos en vigencia para identificar los artículos que pueden requerir de una eliminación segura especial;

c) es posible que sea más fácil realizar las disposiciones necesarias para que se recopilen todos los artículos de medios y que se eliminen de manera segura en vez de intentar separar los artículos sensibles;

d) muchas organizaciones ofrecen servicios de recogida y eliminación de medios; se debería tener cuidado al seleccionar a una parte externa adecuada que cuente con la experiencia y los controles necesarios;

e) la eliminación de los artículos sensibles se debería registrar para mantener un seguimiento de auditoría.

Al acumular medios para su eliminación, se debería tener en consideración el efecto de agregación, que puede hacer que una gran cantidad de información no sensible se vuelva sensible.

Otra información

Es posible que los dispositivos dañados que contienen datos sensibles requieran una evaluación de riesgos para determinar si éstos se deberían destruir físicamente en vez de repararlos o eliminarlos (ver 11.2.7).

8.3.3 Transferencia de medios físicos

Control

Los medios que contienen información deberían estar protegidos contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para proteger a los medios que contienen información que se transporta:

a) se deberían utilizar servicios de transporte o courier confiables;

b) se debería establecer una lista de servicios de courier autorizados con la dirección;

c) se deberían desarrollar procedimientos para verificar la identificación de servicios de courier;

d) el empaque debería ser suficiente para proteger los contenidos de daños físicos que probablemente ocurran durante el tránsito de acuerdo con las especificaciones del fabricante, por ejemplo, protección contra factores ambientales que puede reducir la efectividad de la restauración de los medios, como la exposición al calor, a la humedad y a los campos electromagnéticos;

e) se deberían mantener registros, identificando el contenido de los medios, la protección aplicada, así como también un registro de las veces en que se transfirió a los custodios en tránsito y un recibo en el lugar del destino.

Otra información

La información puede ser vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico al enviar los medios a través del servicio postal o courier. En este control, los medios incluyen a los documentos en papel.

Cuando la información confidencial en los medios no está cifrada, se debería considerar una protección adicional de los medios.

9 Control de acceso

9.1 Requisitos comerciales del control de acceso

Objetivo: limitar el acceso a la información y a las instalaciones de procesamiento de la información.

9.1.1 Política de control de acceso

Control

Se debería establecer, documentar y revisar una política de control de acceso en base a los requisitos del negocio y de la seguridad de la información.

Orientación sobre la implementación

Los propietarios de los activos deberían determinar las reglas de control de la información, los derechos y restricciones de acceso para los roles específicos de los usuarios hacia sus activos, con una cantidad de detalle y rigor en los controles que refleje los riesgos de seguridad de la información asociados.

Los controles de acceso son tanto lógicos como físicos (ver cláusula 11) y éstos se deberían considerar en conjunto. Los usuarios y los proveedores de servicios deberían contar con una declaración clara sobre los requisitos del negocio que se deberían cumplir con los controles de acceso.

La política debería considerar lo siguiente:

a) los requisitos de seguridad de las aplicaciones comerciales;

b) las políticas para la diseminación y autorización de la información, es decir el principio que se debería conocer y los niveles de seguridad de la información y la clasificación de ésta (ver 8.2);

c) coherencia entre los derechos de acceso y las políticas de clasificación de la información de los sistemas y redes;

d) legislación pertinente y cualquier tipo de obligación contractual en cuanto a la limitación de acceso a los datos o servicios (ver 18.1);

e) administración de los derechos de acceso en un entorno de red distribuido que reconozca todos los tipos de conexiones disponibles;

f) segregación de los roles de control de acceso, es decir solicitud de acceso, autorización de acceso y administración de acceso;

g) requisitos de autorización formal para las solicitudes de acceso (ver 9.2.1 y 9.2.2);

h) requisitos de revisión periódicos para los derechos de acceso (ver 9.2.5);

i) eliminación de derechos de acceso (ver 9.2.6);

j) archivo de los registros de todos los eventos de importancia que involucran el uso y la administración de identidades de usuario e información de autenticación secreta;

k) funciones con acceso privilegiado (ver 9.2.3).

Otra información

Se debería tener cuidado al especificar las reglas de control de acceso para considerar lo siguiente:

a) establecer las reglas en base a la premisa “Generalmente todo está prohibido a menos que se permita expresamente” en vez de la regla más débil “Generalmente todo se permite a menos que se prohíba expresamente”;

b) cambios en las etiquetas de información (ver 8.2.2) que se inician automáticamente en las instalaciones de procesamiento de la información y aquellas iniciadas a discreción del usuario;

c) los cambios en los permisos del usuario que inicia automáticamente el sistema de información y los iniciados por un administrador;

d) normas que requieren de aprobación específica antes de su promulgación y las que no.

Las normas de control de acceso se deberían respaldar con procedimientos formales (ver 9.2, 9.3, 9.4) y responsabilidades definidas (ver 6.1.1, 9.3).

El control de acceso basado en roles es un enfoque que se utiliza correctamente en muchas organizaciones para vincular los derechos de acceso con las funciones del negocio.

Dos de los principios frecuentes que dirigen a la política de control de acceso son:

a) Se debería conocer: solo se otorga acceso a la información que necesita para realizar sus tareas (las distintas tareas/roles se traducen en distintas cosas que se deberían conocer y, por lo tanto, en distintos perfiles de acceso);

b) Se debería utilizar: solo se otorga acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos, salas) necesarias para realizar su tarea/trabajo/rol.

9.1.2 Acceso a redes y servicios de red

Control

Los usuarios solo deberían tener acceso a la red y a los servicios de red en los que cuentan con autorización específica.

Orientación sobre la implementación

Se debería formular una política en cuanto al uso de redes y servicios de red. Esta política debería cubrir:

a) las redes y los servicios de red a los que se tiene derecho de acceso;

b) procedimientos de autorización para determinar a quién se le permite acceder a qué redes y servicios con redes;

c) controles y procedimientos de administración para proteger el acceso a las conexiones de red y a los servicios de red;

d) los medios que se utilizan para acceder a las redes y a los servicios con redes (es decir, el uso de VPN o red inalámbrica);

e) requisitos de autenticación del usuario para acceder a los distintos servicios de red;

f) monitoreo del uso de servicios de red.

La política sobre el uso de servicios de red debería ser coherente con la política de control de acceso de la organización (ver 9.1.1).

Otra información

Las conexiones no autorizadas y no seguras a los servicios de red pueden afectar a toda la organización. Este control es de particular importancia para las conexiones de red a aplicaciones comerciales sensibles o críticas o para los usuarios en ubicaciones de alto riesgo, es decir, las áreas públicas o externas que se encuentran fuera de la administración y control de seguridad de la información de la organización.

9.2 Administración de acceso a los usuarios

Objetivo: garantizar el acceso autorizado a los usuarios y evitar el acceso no autorizado a los sistemas y servicios.

9.2.1 Registro y cancelación de registro de usuarios

Control

Se debería implementar un proceso formal de registro y cancelación de registro de un usuario para permitir la asignación de derechos de acceso.

Orientación sobre la implementación

El proceso para administrar IDs de usuario debería incluir:

a) uso de IDs de usuario únicas para permitirle a los usuarios estar vinculados y hacerlos responsables de sus acciones; el uso de IDs compartidas solo se debería permitir donde sea necesario por motivos comerciales u operacionales y se debería aprobar y documentar;

b) deshabilitar o eliminar inmediatamente las IDs de usuario de los usuarios que han abandonado la organización (ver 9.2.6);

c) identificar periódicamente y eliminar o deshabilitar IDs de usuario redundantes;

d) asegurarse de que las IDs de usuario redundantes no se emitan a otros usuarios.

Otra información

La entrega o revocación del acceso a la información o a las instalaciones de procesamiento de información generalmente es un proceso de dos pasos:

a) asignar y habilitar o revocar una ID de usuario;

b) proporcionar o revocar derechos de acceso a dicha ID de usuario (ver 9.2.2).

9.2.2 Entrega de acceso a los usuarios

Control

Se debería implementar un proceso formal de entrega de acceso a los usuarios para asignar o revocar derechos de acceso para todos los tipos de usuario y todos los sistemas y servicios.

Orientación sobre la implementación

El proceso de asignación o revocación de los derechos de acceso que se asignan a las IDs de usuarios debería incluir:

a) obtención de autorización del propietario del sistema o servicio de información para el uso del sistema o servicio de información (ver 8.1.2); también puede resultar adecuada la aprobación por separado de los derechos de acceso de parte de la dirección;

b) verificar que el nivel de acceso otorgado es adecuado para las políticas de acceso (ver 9.1) y que es coherente con otros requisitos como la segregación de deberes (ver 6.1.2);

c) asegurarse de que los derechos de acceso no estén activados (es decir, por los proveedores de servicio) antes de que finalicen los procedimientos de autorización;

d) mantener un registro central de los derechos de acceso otorgados a las IDs de usuario para acceder a los sistemas y servicios de información;

e) adaptar los derechos de acceso de los usuarios que han cambiado de roles o trabajo y eliminar o bloquear inmediatamente los derechos de acceso a los usuarios que han abandonado la organización;

f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas o servicios de información (ver 9.2.5).

Otra información

Se debería considerar establecer roles de acceso de usuario en base a los requisitos del negocio que resuman una cantidad de derechos de acceso en perfiles típicos de acceso de usuarios. Las solicitudes y revisiones de acceso (ver 9.2.4) se manejan más fácilmente al nivel de dichos roles en vez de al nivel de los derechos particulares.

Se debería considerar la inclusión de cláusulas en los contratos del personal y en los contratos de servicio que especifiquen sanciones en el caso de que el personal o los contratistas intenten el acceso no autorizado (ver 7.1.2, 7.2.3, 13.2.4, 15.1.2).

9.2.3 Administración de derechos de acceso privilegiado

Control

La asignación y el uso de derechos de acceso privilegiado se debería restringir y controlar.

Orientación sobre la implementación

La asignación de derechos de acceso privilegiados se debería controlar mediante un proceso de autorización formal de acuerdo con la política de control de acceso pertinente (ver 9.1.1). Se deberían considerar los siguientes pasos:

a) se deberían identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, es decir, sistema operativo, sistema de administración de bases de datos junto con cada aplicación y los usuarios a los que se deberían asignar;

b) se deberían asignar derechos de acceso privilegiado a los usuarios en base a su necesidad de uso y en base a eventos de acuerdo con la política de control de acceso (ver 9.1.1), es decir, en base al requisito mínimo para sus roles funcionales;

c) se debería mantener un proceso de autorización y un registro de todos los privilegios asignados. No se deberían otorgar derechos de acceso privilegiado hasta que el proceso de autorización se haya completado;

d) se deberían definir los requisitos para el vencimiento de los derechos de acceso privilegiado;

e) se deberían asignar derechos de acceso privilegiado a una ID de usuario que sean distintos a los que se utilizan para las actividades comerciales regulares. Las actividades comerciales regulares no se deberían realizar desde una ID privilegiada;

f) las competencias de los usuarios con derechos de acceso privilegiado se deberían revisar regularmente para verificar si están conforme a sus labores;

g) se deberían establecer y mantener procedimientos específicos para poder evitar el uso no autorizado de IDs de usuario de administración genérica de acuerdo a las capacidades de configuración de los sistemas;

h) para las IDs de usuario de administración genérica, la confidencialidad de la información de autenticación secreta se debería mantener cuando se comparte (es decir, cambiando las contraseñas frecuentemente y lo más pronto posible cuando un usuario privilegiado abandona o cambia de trabajo, comunicándolas entre los usuarios privilegiados con mecanismos adecuados).

Otra información

El uso inadecuado de los privilegios de administración del sistema (cualquier función o instalación de un sistema de información que permite al usuario anular los controles del sistema o la aplicación) es un factor importante que contribuye a los incumplimientos de los sistemas.

9.2.4 Administración de la información de autenticación secreta de los usuarios

Control

La asignación de la información de autenticación secreta se debería controlar a través de un proceso de administración formal.

Orientación sobre la implementación

El proceso debería incluir los siguientes requisitos:

a) se debería solicitar a los usuarios firmar una declaración en que mantengan la información de autenticación secreta de manera personal y que mantengan la información de autenticación secreta grupal (es decir, compartida) solo dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones de empleo (ver 7.1.2);

b) cuando se requiere que los usuarios mantengan su propia información de autenticación secreta se les debería proporcionar inicialmente información de autenticación secreta temporal segura, que deberían cambiar obligatoriamente en el primer uso;

c) se deberían establecer procedimientos para verificar la identidad de un usuario antes de proporcionar información de autenticación secreta nueva, de reemplazo o temporal;

d) se debería proporcionar información de autenticación secreta temporal a los usuarios de manera segura; se debería evitar el uso de partes externas o mensajes de correo electrónico no protegidos (texto sin cifrar);

e) la información de autenticación secreta temporal debería ser única para una persona y no se debería poder adivinar;

f) los usuarios deberían confirmar la recepción de la información de autenticación secreta;

g) se debería alterar la información de autenticación secreta predeterminada del proveedor luego de la instalación de los sistemas o software.

Otra información

Las contraseñas son un tipo de información de autenticación secreta de uso común y son una forma común de verificar la identidad de un usuario. Otros tipos de información de autenticación secreta son claves criptográficas y otros datos almacenados en tokens de hardware (es decir, tarjetas inteligentes) que producen códigos de autenticación.

9.2.5 Revisión de los derechos de acceso de usuarios

Control

Los propietarios de activos deberían revisar los derechos de acceso de los usuarios a intervalos regulares.

Orientación sobre la implementación

La revisión de los derechos de acceso debería considerar lo siguiente:

a) los derechos de los accesos de usuario se deberían revisar a intervalos regulares y después de cualquier cambio, como un ascenso, descenso o cese de empleo (ver cláusula 7);

b) los derechos de acceso de usuarios se deberían revisar y volver a asignar al pasar de un rol a otro dentro de la misma organización;

c) se deberían revisar las autorizaciones para los derechos de acceso privilegiados en intervalos más frecuentes;

d) se deberían revisar las asignaciones de privilegios en intervalos regulares para garantizar que no se han obtenido privilegios no autorizados;

e) se deberían registrar los cambios a las cuentas con privilegios para su revisión periódica.

Otra información

Este control compensa cualquier posible debilidad en la ejecución de los controles 9.2.1, 9.2.2 y 9.2.6.

9.2.6 Eliminación o ajuste de los derechos de acceso

Control

Los derechos de acceso para todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información se deberían eliminar al término de su empleo, contrato o acuerdo, o se deberían ajustar en caso de realizarse cambios en el empleo.

Orientación sobre la implementación

Luego del cese del empleo, los derechos de acceso de una persona a la información y a los activos asociados con las instalaciones de procesamiento de información y servicios se deberían eliminar o suspender. Esto determinará si es necesario eliminar los derechos de acceso. Los cambios en el empleo se deberían reflejar en la eliminación de todos los derechos de acceso que no se aprobaron para el nuevo empleo. Los derechos de acceso que se deberían eliminar o ajustar incluyen a los de acceso físico y lógico. La eliminación o el ajuste se puede hacer mediante la eliminación, la revocación o el reemplazo de claves, tarjetas de identificación, instalaciones de procesamiento de información o suscripciones. Cualquier documentación que identifique los derechos de acceso de los empleados y contratistas deberían reflejar la eliminación o el ajuste de los derechos de acceso. Si un empleado o parte externa que abandona el negocio tiene contraseñas conocidas para IDs de usuario que permanecen activas, éstas se deberían cambiar luego del cese o cambio del empleo, contrato o acuerdo.

Los derechos de acceso para la información y los activos asociados a las instalaciones de procesamiento de información se deberían reducir o eliminar antes de que el empleo finalice o cambie, en función de la evaluación de factores de riesgo como:

a) si el cese o cambio lo inició el empleado, el usuario externo o la administración y el motivo para ello.

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

c) el valor de los activos actualmente disponibles.

Otra información

En ciertas circunstancias se pueden asignar derechos de acceso en base a su disponibilidad a más personas que el empleado o la parte externa que se retira, es decir, IDs de grupo. En tales circunstancias, se debería eliminar a las personas que se retiran de cualquier lista de acceso a grupos y se deberían realizar todas las disposiciones necesarias para indicarle al resto de los empleados y usuarios externos que no compartan más esta información con la persona que se retira.

En los casos en que la dirección inició el cese del empleo, los empleados o partes externas disgustados pueden corromper deliberadamente la información o bien sabotear las instalaciones de procesamiento de información. En los casos donde las personas renuncian o se desvinculan, se pueden ver tentados a recopilar información para un uso futuro.

9.3 Responsabilidades de los usuarios

Objetivo: hacer que los usuarios sean responsables de proteger su información de autenticación.

9.3.1 Uso de información de autenticación secreta

Control

Se debería exigir al usuario seguir las prácticas de la organización en el uso de información de autenticación secreta.

Orientación sobre la implementación

Se les debería indicar lo siguiente a todos los usuarios:

a) mantener la información de autenticación secreta como confidencial, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad;

b) evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta, a menos que esto se pueda almacenar de manera segura y de que el método de almacenamiento haya sido aprobado (es decir, bóveda de contraseñas);

c) cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso;

d) cuando se utilizan contraseñas como información de autenticación secreta, seleccione contraseñas con una longitud mínima suficiente que tengan las siguientes características:

   1) fáciles de recordar;

   2) no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con la persona, es decir, nombres, números de teléfono y fechas de nacimiento, etc.;

   3) no sean vulnerable a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios);

   4) estén libre de caracteres idénticos consecutivos, que sean todos numéricos o alfabéticos;

   5) si son temporales, se deberían cambiar en el primer inicio de sesión;

e) no se debería compartir la información de autenticación secreta de usuario de una persona;

f) aseguren la protección adecuada de contraseñas cuando se utilicen las contraseñas como información de autenticación secreta en procedimientos de inicio de sesión automatizados y que se almacenen;

g) no se utilice la misma información de autenticación secreta para fines comerciales y no comerciales.

Otra información

La provisión de herramientas como el inicio de sesión único (SSO - Single Sign On) u otras herramientas de administración de información de autenticación reduce la información de autenticación secreta que los usuarios deberían proteger y, por lo tanto, puede aumentar la efectividad de este control. Sin embargo, estas herramientas también pueden aumentar el impacto de la divulgación de información de autenticación secreta.

9.4 Control de acceso de sistemas y aplicaciones

Objetivo: evitar el acceso no autorizado a los sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información

Control

El acceso a la información y a las funciones del sistema de aplicación se debería restringir de acuerdo a la política de control de acceso.

Orientación sobre la implementación

Las restricciones al acceso se deberían basar en requisitos de aplicación de negocios individuales y de acuerdo con la política de control de acceso definida.

Se debería considerar lo siguiente para poder apoyar los requisitos de restricción de acceso:

a) proporcionar menús para controlar el acceso a las funciones del sistema de aplicación;

b) controlar los datos a los que un usuario en particular puede acceder;

c) controlar los derechos de acceso de los usuarios, es decir, de lectura, escritura, eliminación y ejecución;

d) controlar los derechos de acceso de otras aplicaciones;

e) limitar la información contenida en la producción;

f) proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos o sistemas de aplicación.

9.4.2 Procedimientos de inicio de sesión seguros

Control

Cuando lo requiera la política de control de acceso, el acceso a los sistemas y aplicaciones debería estar controlado por un procedimiento de inicio de sesión seguro.

Orientación sobre la implementación

Se debería seleccionar una técnica de autenticación adecuada para corroborar la identidad que un usuario afirma tener. Cuando se requiera un nivel alto de autenticación y verificación de identidad, se deberían utilizar métodos alternativos a las contraseñas, como medios criptográficos, tarjetas inteligentes, tokens, o medios biométricos.

El procedimiento para iniciar sesión en un sistema o aplicación debería estar diseñado para minimizar la posibilidad de acceso no autorizado. El procedimiento de inicio de sesión, por lo tanto, debería divulgar el mínimo de información acerca del sistema o aplicación, para poder evitar proporcionar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de inicio de sesión debería tener las siguientes características:

a) no mostrar identificadores del sistema o de la aplicación hasta que el proceso de inicio de sesión haya finalizado correctamente;

b) mostrar una advertencia de aviso general que indique que solo deberían acceder usuarios autorizados al computador;

c) no proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que pudieran servir de ayuda a un usuario no autorizado;

d) validar la información de inicio de sesión solo al completar todos los datos de entrada. Si surge una condición de error, el sistema no debería indicar qué parte de los datos son correctos o incorrectos;

e) proteger contra los intentos de inicio de sesión forzados;

f) registrar los intentos logrados y los fallidos;

g) activar un evento de seguridad si se detecta un posible intento de transgresión o su logro en los controles de inicio de sesión;

h) mostrar la siguiente información al completar un inicio de sesión correcto:

1) fecha y hora del inicio de sesión correcto anterior;

2) detalles de cualquier intento de inicio de sesión fallido desde el último inicio de sesión correcto;

i) no mostrar una contraseña que se ingresa;

j) no transmitir contraseñas en texto sin cifrar a través de una red;

k) terminar las sesiones inactivas después de un período de inactividad, en especial en ubicaciones de alto riesgo como áreas públicas o externas fuera de la administración de seguridad de la organización o en dispositivos móviles.

l) restringir los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo y reducir la ventana de oportunidad para el acceso no autorizado.

Otra información

Las contraseñas son una forma común de proporcionar identificación y autenticación en base a un secreto que solo conoce el usuario. Lo mismo se puede lograr con medios criptográficos y protocolos de autenticación. La fortaleza de una autenticación de usuario debería corresponder a la clasificación de la información a la que se accederá.

Si las contraseñas se transmiten en texto sin cifrar durante el inicio de sesión a través de una red, las puede capturar un programa "sniffer" que detecta información.

9.4.3 Sistema de administración de contraseñas

Control

Los sistemas de administración de contraseñas deberían ser interactivos y deberían garantizar contraseñas de calidad.

Orientación sobre la implementación

Un sistema de administración de contraseñas debería:

a) forzar el uso de IDs de usuario y contraseñas individuales para mantener la responsabilidad;

b) permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir los errores de entrada;

c) imponer la selección de contraseñas de calidad;

d) obligar a los usuarios a cambiar sus contraseñas al primer inicio de sesión;

e) imponer cambios regulares de contraseñas según sea necesario;

f) mantener un registro de las contraseñas utilizadas anteriormente y evitar su nuevo uso;

g) no mostrar contraseñas en la pantalla mientras se ingresan;

h) almacenar archivos de contraseñas de manera separada de los datos del sistema de aplicación;

i) almacenar y transmitir contraseñas en forma protegida.

Otra información

Algunas aplicaciones requieren que una autoridad independiente asigne contraseñas de usuario; en tales casos, las letras b), d) y e) de la orientación anterior no se aplican. En la mayoría de los casos los usuarios seleccionan y mantienen las contraseñas.

9.4.4 Uso de programas de utilidad privilegiados

Control

El uso de programas de utilidad que pueden ser capaces de anular el sistema y los controles de aplicación se deberían restringir y controlar íntegramente.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para el uso de programas de utilidad que pueden ser capaces de anular los controles del sistema y de la aplicación:

a) uso de procedimientos de identificación, autenticación y autorización para los programas de utilidad;

b) segregación de programas de utilidad de software de aplicaciones;

c) limitación del uso de programas de utilidad al número mínimo práctico de usuarios confiables y autorizados (ver 9.2.3);

d) autorización para programas de utilidad ad hoc;

e) limitación de la disponibilidad de programas de utilidad, es decir, por la duración de un cambio autorizado;

f) registro de todo el uso de los programas de utilidad;

g) definición y documentación de los niveles de autorización para los programas de utilidad;

h) eliminación o deshabilitación de todos los programas de utilidad innecesarios;

i) no dejar los programas de utilidad disponibles a los usuarios que tienen acceso a las aplicaciones de los sistemas donde se requiere la segregación de deberes.

Otra información

La mayoría de las instalaciones de computadores tienen uno o más programas de utilidad que pueden ser capaces de anular los controles del sistema y de la aplicación.

9.4.5 Control de acceso al código de fuente del programa

Control

Se debería restringir el acceso al código de fuente de programas.

Orientación sobre la implementación

El acceso al código de fuente de programas y los elementos asociados (como diseños, especificaciones, planes de verificación y validación) se debería controlar estrictamente, para poder evitar la introducción de funcionalidades no autorizadas y para evitar los cambios no intencionales, así como también, para mantener la confidencialidad de la propiedad intelectual. Para el código de fuente de programas, esto se puede lograr mediante un almacenamiento central controlado de dicho código, de preferencia en bibliotecas de fuente de programas. Por lo tanto, se deberían considerar las siguientes pautas para controlar el acceso a dichas bibliotecas de fuente de programas y poder reducir el potencial de corrupción de programas computacionales:

a) donde sea posible, las bibliotecas de fuente de programas no se deberían mantener en los sistemas operacionales;

b) el código de fuente de programas y las bibliotecas de fuente de programas se deberían administrar de acuerdo a los procedimientos establecidos;

c) el personal de apoyo no debería contar con acceso sin restricción a las bibliotecas de fuente de programas;

d) la actualización de las bibliotecas de fuente de programas y los elementos asociados, junto con la emisión de las fuentes de programas a los programadores solo se debería realizar cuando se haya recibido la autorización correspondiente;

e) las listas de programas se deberían mantener en un entorno seguro;

f) se debería mantener un registro de auditoría de todos los accesos a las bibliotecas de fuente de programas;

g) el mantenimiento y el copiado de bibliotecas de fuente de programas estarán sujetos a procedimientos de control de cambios estrictos (ver 14.2.2).

Si el código de fuente de programa está hecho para ser publicado, se deberían considerar controles adicionales para ayudar a obtener una garantía de su integridad (es decir, firma digital).

10 Criptografía

10.1 Controles criptográficos

Objetivo: garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

10.1.1 Políticas sobre el uso de controles criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Orientación sobre la implementación

Al desarrollar una política criptográfica se debería considerar lo siguiente:

a) el enfoque de administración hacia el uso de controles criptográficos en toda la organización, incluidos los principios generales bajo los que se debería proteger la información comercial;

b) en base a una evaluación de riesgos, se debería identificar el nivel de protección necesario considerando el tipo, la fortaleza y la calidad del algoritmo de cifrado necesario;

c) el uso de cifrado para la protección de información que se transporta a través de medios móviles o extraíbles o a través de líneas de comunicación.

d) el enfoque a la administración de claves, incluidos los métodos para lidiar con la protección de claves criptográficas y la recuperación de la información cifrada en caso claves perdidas, comprometidas o dañadas;

e) los roles y responsabilidades, es decir, quién es responsable de:

   1) la implementación de la política;

   2) la administración de claves, incluida la generación de claves (ver 10.1.2);

f) las normas que se adoptarán para la implementación eficaz en toda la organización (cuál es la solución que se usa para qué procesos comerciales);

g) el impacto del uso de información cifrada en controles que se apoyan en la inspección de contenido (es decir, la detección de malware).

Al implementar la política criptográfica de la organización, se deberían considerar las normativas y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en distintas partes del mundo y a los asuntos del flujo de información cifrada a través de las fronteras (ver 18.1.5).

Se pueden utilizar controles criptográficos para lograr distintos objetivos de seguridad de la información, es decir:

a) confidencialidad: uso de cifrado de la información para proteger la información sensible o crítica, ya sea almacenada o transmitida;

b) integridad/autenticidad: uso de firmas digitales o códigos de autenticación de mensajes para verificar la autenticidad o integridad de la información almacenada o transmitida sensible o crítica;

c) no repudio: uso de técnicas criptográficas para brindar evidencia de la ocurrencia o no ocurrencia de un evento o acción;

d) autenticación: uso de técnicas criptográficas para autenticar a los usuarios y a otras entidades del sistema que solicitan acceso a o realizan transacciones con usuarios, entidades y recursos del sistema.

Otra información

La toma de una decisión respecto de si una solución criptográfica es adecuada se debería considerar como parte del proceso más amplio de evaluación de riesgos y selección de controles. Esta evaluación se puede utilizar para determinar si un control criptográfico es adecuado, qué tipo de control se debería aplicar y para qué propósito y procesos comerciales.

Es necesaria una política sobre el uso de controles criptográficos para maximizar los beneficios y minimizar los riesgos del uso de técnicas criptográficas y para evitar el uso inadecuado o incorrecto.

Se debería buscar la asesoría de especialistas al seleccionar los controles criptográficos adecuados para cumplir con los objetivos de la política de seguridad de la información.

10.1.2 Administración de claves

Control

Se debería desarrollar e implementar una política sobre el uso, la protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.

Orientación sobre la implementación

La política debería incluir los requisitos para administrar claves criptográficas a través de todo su ciclo de vida incluida la generación, el almacenamiento, el archivo, la recuperación, la distribución, el retiro y la destrucción de claves.

Los algoritmos criptográficos, las longitudes de las claves y las prácticas de uso se deberían seleccionar de acuerdo a las buenas prácticas. La administración adecuada de claves requiere de procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves criptográficas.

Todas las claves criptográficas se deberían proteger contra la modificación y las pérdidas. Además, las claves secretas y privadas necesitan de protección contra el uso no autorizado junto con la divulgación. Los equipos que se utilizan para generar, almacenar y archivar claves deberían estar protegidos físicamente.

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

a) generar claves para distintos sistemas criptográficos y distintas aplicaciones;

b) emitir y obtener certificados de claves públicos;

c) distribuir claves a las entidades deseadas, incluida además la forma en que se deberían activar tras su recepción;

d) almacenamiento de claves, incluida la forma en que los usuarios obtienen acceso a las claves;

e) cambio o actualización de claves incluidas las reglas sobre cuando se deberían cambiar las claves y cómo se hará;

f) encargarse de las claves comprometidas;

g) eliminar claves, incluida la forma en que se deberían retirar o desactivar, es decir, cuando se han comprometido las claves o cuando un usuario abandona una organización (en cuyo caso las claves también se deberían archivar);

h) recuperación de las claves pérdidas o corrompidas;

i) respaldo o archivado de claves;

j) destrucción de claves;

k) registro y auditoría de actividades relacionadas con la administración de claves.

Para poder reducir la probabilidad del uso inadecuado, se deberían definir las fechas de activación y desactivación para las claves de modo que solo se puedan utilizar por el período de tiempo definido en la política de administración de claves asociada.

Además de la administración segura de claves secretas y privadas, también se debería considerar la autenticidad de las claves públicas. Este proceso de autenticación se puede realizar utilizando certificados de claves públicos, que generalmente los emite una autoridad de certificación, que debería ser una organización reconocida con controles y procedimientos adecuados en vigencia para proporcionar el nivel de confianza necesario.

El contenido de los acuerdos o contratos de nivel de servicios con proveedores externos o servicios criptográficos, es decir, con una autoridad de certificación, debería cubrir asuntos de confiabilidad de los servicios y tiempos de respuesta para la provisión de servicios (ver 15.2).

Otra información

La administración de claves criptográficas es fundamental para el uso eficaz de las técnicas criptográficas.

ISO/IEC 11770 brinda más información sobre la administración de claves.

También se pueden utilizar técnicas criptográficas para proteger claves criptográficas. Es posible que se deban considerar procedimientos para manejar las solicitudes legales para el acceso a claves criptográficas, es decir, se puede requerir tener disponible información de manera descifrada como evidencia en un caso de tribunales.

11 Seguridad física y ambiental

11.1 Areas seguras

Objetivo: evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización y las instalaciones de procesamiento de la información.

11.1.1 Perímetro de seguridad física

Control

Los perímetros de seguridad se deberían definir y utilizar para proteger a las áreas que contienen información y a las instalaciones de procesamiento de información sensible o crítica.

Orientación sobre la implementación

Las siguientes pautas se deberían considerar e implementar donde corresponda para los perímetros de seguridad físicos:

a) se deberían definir perímetros de seguridad y el emplazamiento y la ubicación de cada uno de los perímetros debería depender de los requisitos de seguridad de los activos dentro del perímetro y los resultados de una evaluación de riesgos;

b) los perímetros del edificio o del sitio donde se albergan las instalaciones de procesamiento de información deberían ser físicamente sólidos (es decir, no deberían haber brechas en el perímetro o en las áreas donde se podría generar un agrietamiento fácilmente); el techo exterior, las paredes y el piso del sitio deberían ser de construcción sólida y todas las puertas externas deberían estar protegidas adecuadamente contra el acceso no autorizado con mecanismos de control, (es decir, barras, alarmas, candados); las puertas y ventanas se deberían cerrar con llave correctamente, cuando se dejan sin vigilancia y se debería considerar una protección externa para las ventanas, en particular a nivel del suelo;

c) se debería contar con un área de recepción atendida por una persona u otros medios para controlar el acceso físico al sitio o al edificio; el acceso a los sitios y al edificio se debería restringir solo al personal autorizado;

d) se deberían construir barreras físicas donde corresponda para evitar el acceso físico no autorizado y la contaminación ambiental;

e) todas las puertas contra incendios en un perímetro de seguridad deberían tener una alarma, ser monitoreadas y probadas en conjunto con las paredes para establecer el nivel de resistencia necesario de acuerdo con las normas regionales, nacionales e internacionales correspondientes; deberían operar de acuerdo al código de incendios local y a prueba de fallos;

f) se deberían instalar sistemas de detección de intrusos adecuados de acuerdo con las normas nacionales, regionales o internacionales y se deberían probar regularmente para cubrir todas las puertas externas y las ventanas accesibles; las áreas no ocupadas deberían tener las alarmas activadas en todo momento; también se debería proporcionar una cubierta para el resto de las áreas, es decir, las salas de computación o las salas de comunicaciones;

g) las instalaciones de procesamiento de información que administra la organización deberían estar separada físicamente de las que administran terceros.

Otra información

Se puede lograr protección al crear una o más barreras físicas alrededor de las dependencias y las instalaciones de procesamiento de información de la organización. El uso de varias barreras brinda protección adicional, donde la falla de una sola barrera no significa que la seguridad se ve comprometida inmediatamente.

El área segura puede ser una oficina que se puede cerrar con llave o varias salas rodeadas de una barrera de seguridad física interna continua. Es posible que se necesiten barreras y perímetros adicionales para controlar el acceso físico entre las áreas con distintos requisitos de seguridad dentro del perímetro de seguridad. Se debería prestar especial atención a la seguridad del acceso físico en el caso de los edificios que albergan activos para varias organizaciones.

La aplicación de controles físicos, en especial para las áreas seguras, se debería adaptar a las circunstancias técnicas y económicas de la organización, según se establece en la evaluación de riesgos.

11.1.2 Controles de entrada física

Control

Las áreas seguras deberían estar protegidas con controles de entrada adecuados para garantizar que solo se permita el acceso al personal autorizado.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas:

a) se debería registrar la fecha y la hora de entrada y salida de las visitas y, se debería supervisar a todas las visitas a menos que su acceso haya sido aprobado anteriormente; solo se les debería otorgar acceso para propósitos específicos y autorizados y se debería emitir de acuerdo a las instrucciones de los requisitos de seguridad del área y a los procedimientos de emergencia. Se debería autenticar la identidad de las visitas con un medio adecuado;

b) el acceso a las áreas donde se procesa o almacena la información confidencial se debería restringir a las personas autorizadas solo mediante la implementación de controles de acceso adecuados, es decir, al implementar un mecanismo de autenticación de dos factores como una tarjeta de acceso y un PIN secreto;

c) se debería mantener y monitorear de manera segura un libro de registro físico o una auditoría de seguimiento electrónica de todo el acceso;

d) todos los empleados, contratistas y partes externas deberían portar algún tipo de identificación visible y se debería notificar inmediatamente al personal de seguridad si encuentran visitas sin escolta y a cualquier persona que no porte una identificación visible;

e) se le debería otorgar acceso restringido al personal de servicios de apoyo de terceros a las áreas seguras o a las instalaciones de procesamiento de información confidencial solo cuando sea necesario; este acceso se debería autorizar y monitorear;

f) los derechos de acceso a las áreas protegidas se deberían revisar y actualizar de manera regular y, revocar cuando sea necesario (ver 9.2.5 y 9.2.6).

11.1.3 Protección de oficinas, salas e instalaciones

Control

Se debería diseñar y aplicar un sistema de seguridad física para las oficinas, salas e instalaciones.

Orientación sobre la implementación

Las siguientes pautas se deberían considerar para proteger a las oficinas, salas e instalaciones:

a) las instalaciones clave se deberían emplazar para evitar el acceso del público;

b) donde corresponda, los edificios deberían ser discretos y brindar una indicación mínima sobre su propósito, sin signos obvios, fuera o dentro del edificio, identificando la presencia de actividades de procesamiento de información;

c) las instalaciones se deberían configurar para evitar que la información o las actividades confidenciales se vean y escuchen desde fuera. También se debería considerar el blindaje electromagnético como adecuado;

d) los directorios y las libretas telefónicas internas que identifican la ubicación de las instalaciones de procesamiento de información confidencial no deberían estar disponibles fácilmente a personas no autorizadas.

11.1.4 Protección contra las amenazas externas y ambientales

Control

Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Orientación sobre la implementación

Se debería obtener asesoría de especialistas sobre cómo evitar los daños provocados por incendios, inundaciones, terremotos, explosiones, disturbios y otras formas de desastres naturales o provocados por el hombre.

11.1.5 Trabajo en áreas seguras

Control

Se deberían diseñar y aplicar procedimientos para trabajar en áreas seguras.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas:

a) el personal debería estar al tanto de la existencia de, o de las actividades dentro de un área segura según se considere necesario.

b) se debería evitar el trabajo no supervisado en áreas seguras, tanto por motivos de seguridad como para evitar las oportunidades de actividades maliciosas;

c) las áreas seguras vacantes se deberían cerrar físicamente con candado y se deberían revisar de manera periódica;

d) no se deberían permitir los equipos fotográficos, de video o audio, como las cámaras de dispositivos móviles, a menos que se autoricen.

Las disposiciones para trabajar en áreas seguras incluyen controles para los empleados y usuarios de terceros trabajando en el área segura y cubren todas las actividades que se realizan en el área segura.

11.1.6 Areas de entrega y carga

Control

Se deberían controlar los puntos de acceso como las áreas de entrega y carga y otros puntos donde pudieran ingresar personas no autorizadas a las dependencias y, de ser posible, se deberían aislar de las instalaciones de procesamiento de información para evitar el acceso.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas:

a) se debería restringir el acceso a un área de entrega y carga desde fuera del edificio al personal identificado y autorizado;

b) el área de entrega y carga debería estar diseñado de manera que se puedan cargar y descargar los suministros sin que el personal que realiza la entrega acceda a otras áreas del edificio;

c) las puertas externas a un área de entrega y carga se deberían resguardar cuando se abren las puertas internas;

d) se debería inspeccionar y examinar el material entrante en busca de explosivos, químicos u otros materiales peligrosos, antes de que se mueva de un área de entrega y carga;

e) el material entrante se debería registrar de acuerdo con los procedimientos de administración de activos (ver cláusula 8) en la entrada al sitio;

f) los envíos entrantes y salientes se deberían segregar físicamente, donde sea posible;

g) se debería inspeccionar al material entrante en busca de evidencias de manipulación indebida en la ruta. Si se descubre la manipulación, se debería informar inmediatamente al personal de seguridad.

11.2 Equipos

Objetivo: evitar la pérdida, los daños, el robo o el compromiso de activos y la interrupción a las operaciones de la organización.

11.2.1 Emplazamiento y protección de equipos

Control

Los equipos se deberían emplazar y proteger para reducir los riesgos de las amenazas y peligros ambientales y las oportunidades de acceso no autorizado.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para la protección de equipos:

a) el equipo se debería emplazar en un lugar determinado para minimizar el acceso innecesario a las áreas de trabajo;

b) las instalaciones de procesamiento de información que manejan datos sensibles se deberían ubicar cuidadosamente para reducir el riesgo de que personas no autorizadas la vean durante su uso;

c) las instalaciones de almacenamiento se deberían proteger para evitar el acceso no autorizado;

d) los elementos que requieren protección especial se deberían resguardar para reducir el nivel general de protección necesaria;

e) se deberían adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, es decir, robos, incendios, humo, agua (o una falla del suministro de agua), polvo, vibraciones, efectos químicos, interferencia del suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;

f) se deberían establecer pautas para comer, beber y fumar en la proximidad de las instalaciones de procesamiento de información;

g) se deberían monitorear las condiciones ambientales como la temperatura y la humedad en busca de condiciones que pudieran afectar adversamente a la operación de las instalaciones de procesamiento de información;

h) se debería aplicar protección a la luminaria en todos los edificios y se deberían instalar filtros de protección de iluminación a todas los cables de tendido eléctrico y de comunicación entrantes;

i) se debería considerar el uso de métodos de protección especial, como membranas de teclado para los equipos en entornos industriales;

j) la información confidencial del procesamiento de equipos se debería proteger para minimizar el riesgo del filtrado de información debido a la emanación electromagnética.

11.2.2 Servicios básicos de apoyo

Control

El equipo debería estar protegido contra cortes de luz y otras interrupciones provocadas por fallas en los servicios básicos de apoyo.

Orientación sobre la implementación

Los servicios básicos de apoyo (es decir, la electricidad, las telecomunicaciones, el suministro de agua, gas, ventilación y aire acondicionado) deberían:

a) cumplir con las especificaciones del fabricante del equipo y con los requisitos legales locales;

b) someterse a evaluaciones periódicas para cumplir con el crecimiento del negocio y las interacciones con otros servicios básicos de apoyo;

c) someterse a inspecciones y pruebas regularmente para garantizar su funcionamiento correcto;

d) en caso de ser necesario contar con alarmas para detectar fallas;

e) en caso de ser necesario, debería contar con varias alimentaciones con distintos enrutamientos físicos.

Se deberían proporcionar iluminación y comunicaciones de emergencia. Los interruptores de emergencia y las válvulas para cortar la electricidad, el agua, el gas u otros servicios básicos se deberían ubicar cerca de las salidas de emergencia o de las salas equipadas.

Otra información

Se puede obtener una redundancia adicional para la conectividad de redes mediante varias rutas de más de un proveedor de servicios básicos.

11.2.3 Seguridad del cableado

Control

Los cables de electricidad y telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger de la intercepción, interferencia o daños.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para la seguridad del cableado:

a) los cables de electricidad y telecomunicaciones hacia las instalaciones de procesamiento de información deberían ser subterráneos, donde sea posible o estar sujetos a protección alternativa adecuada;

b) los cables de electricidad deberían estar apartados de los cables de comunicación para evitar interferencias;

c) para los sistemas sensibles o críticos, se deberían considerar más controles que incluyen:

   1) la instalación de conductos armados y salas o cajas cerradas con llave en los puntos de inspección y terminación;

   2) el uso de blindaje electromagnético para proteger los cables;

   3) el inicio de barridas técnicas e inspecciones físicas en busca de dispositivos no autorizados conectados a los cables;

   4) el acceso controlado a los paneles de parches y a las salas de cables.

11.2.4 Mantenimiento de equipos

Control

Los equipos se deberían mantener correctamente para garantizar su disponibilidad e integridad continuas.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para el mantenimiento de equipos:

a) los equipos se deberían mantener de acuerdo a los intervalos y especificaciones de servicio recomendados por el proveedor;

b) solo el personal de mantenimiento autorizado debería realizar reparaciones y labores de mantenimiento y servicio a los equipos;

c) se deberían mantener registros de todas las fallas sospechosas o reales y de todo el mantenimiento preventivo y correctivo;

d) se deberían implementar controles adecuados cuando se programa el mantenimiento de equipos considerando si este mantenimiento lo realizará el personal en terreno o externo a la organización; donde sea necesario se debería eliminar la información confidencial del equipo o bien lo debería realizar el personal de mantenimiento;

e) se debería cumplir con todos los requisitos de mantenimiento impuestos por las políticas de seguros;

f) luego de volver a poner al equipo en funcionamiento después de su mantenimiento, se debería inspeccionar para garantizar que no ha sido adulterado y que funciona adecuadamente.

11.2.5 Retiro de activos

Control

Los equipos, la información o el software no se deberían retirar del sitio sin una autorización previa.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas:

a) se debería identificar a los empleados y partes externas que tienen la autoridad para permitir el retiro fuera del sitio de los activos;

b) se deberían establecer límites de tiempo para el retiro de activos y los retornos se deberían verificar para comprobar su cumplimiento;

c) donde sea necesario y corresponda, se deberían registrar a los activos que se retiran del sitio y también cuando se regresan;

d) la identidad, el rol y la afiliación de cualquier persona que maneje o utilice activos se debería documentar y, esta documentación se debería regresar con el equipo, la información o el software.

Otra información

Las comprobaciones rápidas que se realizan para detectar el retiro no autorizado de activos, también se pueden realizar para detectar dispositivos de grabación no autorizados, armas, etc. y para evitar su ingreso y egreso desde el sitio. Dichas comprobaciones rápidas se deberían realizar de acuerdo con la legislación y normativas pertinentes. Las personas deberían estar en conocimiento de la realización de las comprobaciones rápidas y las verificaciones solo se deberían realizar con la autorización correspondiente de acuerdo con los requisitos legales y normativos.

11.2.6 Seguridad de los equipos y los activos fuera de las dependencias

Control

Se debería aplicar la seguridad fuera del sitio a los activos considerando los distintos riesgos de trabajar fuera de las dependencias de la organización.

Orientación sobre la implementación

El uso de cualquier tipo de equipos de almacenamiento y procesamiento de información fuera de las dependencias de la organización debería autorizarlo la dirección. Esto se aplica a los equipos de propiedad de la organización y a los equipos de propiedad privada que se utilizan a nombre de la organización.

Se deberían considerar las siguientes pautas para la protección del equipo fuera del sitio:

a) los equipos y medios que se sacan de las dependencias no se deberían dejar sin supervisión en lugares públicos;

b) se deberían observar las instrucciones del fabricante en todo momento, es decir, la protección contra la exposición a campos electromagnéticos fuertes;

c) se deberían determinar controles para las ubicaciones fuera de las dependencias, como el trabajo en casa, el teletrabajo y los sitios temporales mediante una evaluación de riesgos y se deberían aplicar los controles adecuados según corresponda, es decir, archivadores con llave, política de escritorio despejado, controles de acceso para los computadores y comunicación segura con la oficina (ver también ISO/IEC 27033);

d) cuando se trasladan los equipos fuera de las dependencias entre distintas personas o partes externas, se debería mantener un registro que defina la cadena de custodia para el equipo incluidos al menos los nombres y las organizaciones de aquellos responsables de los equipos.

Los riesgos, es decir, los daños, el robo, el escuchar secretamente pueden variar considerablemente entre las ubicaciones y se deberían considerar al determinar los controles más adecuados.

Otra información

Los equipos de almacenamiento y procesamiento de información incluyen todas las formas de computadores personales, organizadores, teléfonos móviles, tarjetas inteligentes, papel u otra forma, que se mantiene para el trabajo en casa o para transportarla fuera de la ubicación de trabajo normal.

Puede encontrar más información sobre otros aspectos de la protección de equipos móviles en 6.2.

Puede resultar adecuado evitar el riesgo desalentando a ciertos empleados a trabajar fuera del sitio o restringir su uso de equipos de TI portátil;

11.2.7 Eliminación o reutilización segura de equipos

Control

Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Orientación sobre la implementación

Se debería verificar el equipo para asegurarse de que contiene o no medios de almacenamiento antes de su eliminación o reutilización. Los medios de almacenamiento que contienen información confidencial o con derecho de autor se deberían destruir físicamente o bien, la información se debería destruir, eliminar o sobrescribir mediante técnicas para hacer que la información original no se pueda recuperar en vez de utilizar la función de eliminación o formateo normal.

Otra información

Es posible que los equipos dañados que contienen medios de almacenamiento requieran una evaluación de riesgos para determinar si éstos se deberían destruir físicamente en vez de repararlos o eliminarlos. La información se puede ver comprometida a través de la eliminación o la reutilización de equipos poco cuidadosa.

Además del borrado seguro del disco, el cifrado del disco completo reduce el riesgo de divulgar información confidencial cuando se elimina o vuelve a implementar el equipo, siempre que:

a) el proceso de cifrado sea lo suficientemente fuerte y que cubra a todo el disco (incluido el espacio despejado, los archivos de intercambio, etc.);

b) las claves de cifrado sean lo suficientemente largas como para resistir los ataques de fuerza bruta;

c) las claves de cifrado en sí se mantengan de manera confidencial (es decir, que nunca se almacenen en el mismo disco).

Para obtener más información sobre el cifrado, ver cláusula 10.

Las técnicas para sobrescribir los medios de almacenamiento de manera segura pueden diferir de acuerdo con la tecnología de los medios de almacenamiento. Se deberían revisar las herramientas de sobreescritura para asegurarse de que se pueden aplicar a la tecnología de los medios de almacenamiento.

11.2.8 Equipos de usuario no supervisados

Control

Los usuarios se deberían asegurar de que los equipos no supervisados cuentan con la protección adecuada.

Orientación sobre la implementación

Todos los usuarios deberían conocer los requisitos y procedimientos de seguridad para proteger a los equipos sin supervisión, así como también sus responsabilidades para implementar dicha protección. Se les debería indicar lo siguiente a los usuarios:

a) que finalicen las sesiones activas cuando terminen, a menos que se puedan proteger con un mecanismo de bloqueo adecuado, es decir, un protector de pantalla protegido con contraseña;

b) cerrar sesión en las aplicaciones o servicios de redes cuando ya no se necesiten;

c) proteger a los computadores o dispositivos móviles del uso no autorizado mediante un candado con llave o un control equivalente, es decir, acceso con contraseña, cuando no se utilice.

11.2.9 Política de escritorio despejado y pantalla despejada

Control

Se debería adoptar una política de escritorio despejado para los papeles y para los medios de almacenamiento extraíbles y una política de pantalla despejada para las instalaciones de procesamiento de información.

Orientación sobre la implementación

La política de escritorio despejado y pantalla despejada debería considerar las clasificaciones de información (ver 8.2), los requisitos legales y contractuales (ver 18.1) y los riesgos y aspectos culturales correspondientes de la organización. Se deberían considerar las siguientes pautas:

a) la información sensible o crítica para el negocio, es decir, en medios de almacenamiento electrónico o papel, se debería mantener guardada bajo llave (idealmente en una caja fuerte o gabinete u otras formas de muebles de seguridad) cuando no se necesite, especialmente cuando la oficina esté desocupada.

b) se deberían mantener desconectados a los computadores y terminales o protegidos con un mecanismo de bloqueo de pantalla y teclado mediante una contraseña, token o mecanismo de autenticación de usuario similar cuando se deja sin supervisar y se debería proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso;

c) se debería evitar el uso no autorizado de fotocopiadoras u otro tipo de tecnologías de reproducción (es decir, escáneres, cámaras digitales);

d) los medios que contienen información sensible o clasificada se deberían extraer de las impresoras inmediatamente.

Otra información

Una política de escritorio despejado/pantalla despejada reduce el riesgo del acceso al personal no autorizado, la pérdida o daño de la información durante y fuera de las horas laborales normales. Las cajas fuertes y otras formas de instalaciones de almacenamiento seguro también pueden proteger a la información almacenada en su interior contra desastres como incendios, terremotos, inundaciones o explosiones.

Considere el uso de impresoras con función de código PIN, para que los originadores sean los únicos que puedan obtener sus impresiones y solo al estar al lado de la impresora.

12 Seguridad de las operaciones

12.1 Procedimientos y responsabilidades operacionales

Objetivo: garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos operativos documentados

Control

Los procedimientos operativos se deberían documentar y dejar a disposición de todos los usuarios que los necesiten.

Orientación sobre la implementación

Se deberían preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación de información, como procedimientos de inicio y cierre de sesión de computadores, respaldo, mantenimiento de equipos, manejo de medios, salas de computación y administración y seguridad de manejo de correo.

Los procedimientos operativos deberían especificar las instrucciones operacionales, incluidas:

a) la instalación y configuración de los sistemas;

b) el procesamiento y manipulación de la información tanto automática como manual;

c) respaldo (ver 12.3);

d) los requisitos de programación, incluidas las interdependencias con otros sistemas, las horas de inicio del trabajo más temprano y de finalización del trabajo más tardías;

e) instrucciones para el manejo de errores u otras condiciones excepcionales, los que pueden surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de las utilidades del sistema (ver 9.4.4);

f) contactos de apoyo y escalamiento incluidos los contactos de soporte externos en el caso de presentarse dificultades operativas o técnicas inesperadas;

g) instrucciones de manejo de salidas y medios especiales, como el uso de papelería especial o el manejo de resultados confidenciales incluidos los procedimientos para la eliminación segura de salidas de trabajos fallidos (ver 8.3 y 11.2.7);

h) reinicio del sistema y procedimientos de recuperación para utilizar en el caso de fallas del sistema;

i) la administración del seguimiento de auditoría y de la información de registro del sistema (ver 12.4);

j) procedimientos de monitoreo.

Los procedimientos operativos y los procedimientos documentados para las actividades del sistema se deberían tratar como documentos formales y los cambios deberían estar autorizados por la dirección. Donde sea técnicamente factible, los sistemas de información se deberían administrar de manera coherente, utilizando los mismos procedimientos, herramientas y utilidades.

12.1.2 Administración de cambios

Control

Se deberían controlar los cambios a la organización, los procesos comerciales, las instalaciones de procesamiento de información y los sistemas que afectan a la seguridad de la información.

Orientación sobre la implementación

En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de cambios significativos;

b) planificación y pruebas de cambios;

c) evaluación de los posibles impactos, incluidos los impactos de seguridad en la información, de dichos cambios;

d) procedimiento de aprobación formal para los cambios propuestos;

e) verificación de que se han cumplido los requisitos de seguridad;

f) comunicación de los detalles de los cambios a todas las personas pertinentes;

g) procedimientos de retroceso, incluidos los procedimientos y responsabilidades para abortar y recuperar los cambios incorrectos y los eventos inesperados;

h) provisión de un proceso de cambio de emergencia para permitir la implementación rápida y controlada de los cambios necesarios para resolver un incidente (ver 16.1).

Deberían existir responsabilidades y procedimientos de administración formales para garantizar el control satisfactorio de todos los cambios. Cuando se realizan los cambios, se debería mantener un registro de auditoría que contenga toda la información pertinente.

Otra información

El control inadecuado de cambios a las instalaciones y sistemas de procesamiento de la información es una causa común para las fallas de seguridad o del sistema. Los cambios al entorno operacional, especialmente al transferir un sistema desde la etapa de desarrollo a la operacional, pueden tener un impacto en la fiabilidad de las aplicaciones (ver 14.2.2).

12.1.3 Administración de capacidad

Control

El uso de recursos se debería monitorear, ajustar y se deberían hacer las proyecciones necesarias para los requisitos futuros de capacidad y así poder garantizar el rendimiento que el sistema requiere.

Orientación sobre la implementación

Se deberían identificar los requisitos de capacidad, considerando la criticidad para el negocio del sistema involucrado. Se debería aplicar el procedimiento de ajuste y monitoreo del sistema para garantizar y, donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Se deberían poner controles de detección en vigencia para indicar los problemas a su debido tiempo. Las proyecciones sobre los requisitos futuros de capacidad deberían considerar los nuevos requisitos del negocio y del sistema y las tendencias actuales y proyectadas en las capacidades de procesamiento de información de la organización.

Se debería prestar especial atención a cualquier recurso con tiempos de acción de adquisición extensos o costos altos, por lo tanto, los gerentes deberían monitorear la utilización de los recursos de los sistemas clave. Deberían identificar las tendencias en el uso, en particular en relación con las aplicaciones comerciales o con las herramientas de administración de sistemas de información.

Los gerentes deberían utilizar esta información para identificar y evitar posibles cuellos de botella y la dependencia del personal clave que puede presentar una amenaza a la seguridad o los servicios del sistema y planificar acciones adecuadas.

Se puede proporcionar una capacidad suficiente mediante el aumento de la capacidad o la reducción de la demanda. Algunos ejemplos de la administración de la demanda de capacidad incluyen:

a) eliminación de datos obsoletos (espacio en el disco);

b) sacar de servicio a las aplicaciones, sistemas, bases de datos o entornos;

c) eliminación de los procesos y programaciones de parches;

d) optimización de las consultas de lógicas de aplicaciones o bases de datos;

e) negación o restricción del ancho de banda para recursos que consumen muchos recursos si no son críticos para el negocio (es decir, streaming de video).

Se debería considerar un plan de administración de capacidad documentado para los sistemas críticos para la misión.

Otra información

Este control también aborda la capacidad de los recursos humanos, así como también las oficinas e instalaciones.

12.1.4 Separación de entornos de desarrollo, pruebas y operacionales

Control

Los entornos de desarrollo, pruebas y operacionales se deberían separar para reducir los riesgos del acceso o cambios no autorizados al entorno operacional.

Orientación sobre la implementación

Se debería identificar e implementar el nivel de separación entre los entornos operativos, de prueba y desarrollo necesario para evitar los problemas operacionales.

Se deberían considerar los siguientes elementos:

a) se deberían definir y documentar las reglas de transferencia de software desde un estado de desarrollo al operacional;

b) el software de desarrollo y operativo se debería ejecutar en distintos sistemas o procesadores de computador y en distintos dominios y directorios;

c) se deberían probar los cambios a los sistemas operativos y aplicaciones en un entorno de pruebas o etapas antes de aplicarlos a los sistemas operacionales;

d) a no ser que sea bajo circunstancias excepcionales, no se deberían realizar pruebas en los sistemas operativos;

e) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían estar accesibles desde los sistemas operacionales cuando no sea necesario;

f) los usuarios deberían utilizar distintos perfiles de usuario para los sistemas operacionales y de prueba y se deberían mostrar menús para mostrar mensajes de identificación adecuados para reducir el riesgo de errores;

g) los datos sensibles no se deberían copiar en el entorno del sistema de pruebas a menos que se entreguen controles equivalentes para el sistema de pruebas (ver 14.3).

Otra información

Las actividades de desarrollo y pruebas pueden provocar problemas graves, es decir, la modificación no deseada de archivos o del entorno del sistema o una falla del sistema. Existe la necesidad de mantener un entorno conocido y estable en el que se pueden realizar pruebas significativas para evitar el acceso inadecuado del desarrollador al entorno operacional.

Cuando el personal de desarrollo y pruebas tenga acceso al sistema operativo y a su información, podrían introducir un código no autorizado o no probado, o alterar los datos operacionales. En algunos sistemas esta capacidad se podría utilizar incorrectamente para cometer fraudes o introducir un código sin probar o malicioso, lo que puede generar problemas operacionales graves.

El personal de desarrollo y pruebas también representa una amenaza a la confidencialidad de la información operacional. Las actividades de desarrollo y pruebas pueden provocar cambios no intencionados al software o la información si comparten el mismo entorno computacional. Por lo tanto, se aconseja la separación de los entornos desarrollo, de pruebas y operativos para reducir el riesgo de cambios accidentales o del acceso no autorizado al software operacional y los datos del negocio (ver 14.3 para obtener información sobre la protección de los datos de prueba).

12.2 Protección contra malware

Objetivo: garantizar que la información y que las instalaciones de procesamiento de información estén protegidas contra el malware.

12.2.1 Controles contra el malware

Control

Se deberían implementar controles para la detección, prevención y recuperación para resguardarse contra el malware en combinación con la concientización adecuada para los usuarios.

Orientación sobre la implementación

La protección contra el malware se debería basar en controles de software de detección de malware y de reparación, la concientización sobre la seguridad de la información, el acceso adecuado al sistema y la administración de cambios. Se deberían considerar las siguientes pautas:

a) establecer una política formal que prohíbe el uso de software no autorizado (ver 12.6.2 y 14.2.);

b) implementar controles que evitan o detectan el uso de software no autorizado (es decir, la creación de una lista blanca de aplicaciones);

c) implementar controles que eviten o detecten el uso de sitios web desconocidos o que se sospecha son maliciosos (es decir, la elaboración de una lista negra).

d) establecimiento de una política formal para protegerse contra los riesgos asociados al obtener archivos y software ya sea de redes externas o a través de cualquier otro medio, indicando las medidas de protección que se deberían tomar;

e) reducción de las vulnerabilidades que se podrían desencadenar por el malware, es decir, a través de la administración de vulnerabilidades técnicas (ver 12.6);

f) realizar revisiones periódicas del software y del contenido de los datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de cualquier tipo de archivos o modificaciones no autorizados;

g) instalación y actualización periódica de software de detección de malware y reparación para analizar computadores y medios como control de precaución o, de manera rutinaria; el análisis debería incluir:

   1) analizar solo los archivos recibidos a través de redes o mediante cualquier forma de medios de almacenamiento, en busca de malware antes de su uso;

   2) analizar datos adjuntos de correos electrónicos en busca de malware antes de su uso; este análisis se debería realizar en diferentes lugares, es decir, en servidores de correo electrónico, computadores de escritorio y al ingresar a la red de la organización;

   3) analizar páginas web en busca de malware;

h) definir procedimientos y responsabilidades que involucren la protección contra malware en los sistemas, capacitándose sobre su uso, informando sobre y recuperándose ante ataques de malware;

i) preparar planes de continuidad comercial adecuados para recuperarse contra ataques de malware, incluidos todos los datos, respaldo de software y disposiciones de recuperación necesarios (ver 12.3);

j) implementar procedimientos para recopilar información de manera regular, como la suscripción a listas de correo electrónico o verificar los sitios web que brindan información sobre el nuevo malware;

k) implementar procedimientos para verificar la información relacionada al malware y asegurarse de que los boletines de advertencia son precisos e informativos; los gerentes se deberían asegurar de que se utilicen fuentes calificadas, es decir, publicaciones de reconocido prestigio, sitios de internet o proveedores productores de software de protección contra malware confiables para diferenciar entre malware falso y el real; todos los usuarios deberían estar en conocimiento del problema de malware falso y qué hacer en caso de recibirlo;

l) aislar entornos donde pueden se pueden generar impactos catastróficos.

Otra información

El uso de dos o más productos de software que proteja contra malware en todo el entorno de procesamiento de información de distintos proveedores y tecnología puede mejorar la efectividad de la protección contra el malware.

Se debería tener cuidado de protegerse contra la introducción de malware durante los procedimientos de mantenimiento y de emergencia, los que pueden omitir los controles normales de protección contra malware.

Bajo ciertas condiciones, la protección contra malware puede provocar interrupciones dentro de las operaciones.

El uso de software de detección y reparación de malware por sí solo para el control del malware generalmente no resulta adecuado y a menudo se debería acompañar de procedimientos operativos que eviten la introducción de malware.

12.3 Respaldo

Objetivo: brindar protección contra la pérdida de datos.

12.3.1 Respaldo de información

Control

Se deberían realizar copias de la información, del software y de las imágenes del sistema y se deberían probar de manera regular de acuerdo con una política de respaldo acordada.

Orientación sobre la implementación

Se debería establecer una política de respaldo para definir los requisitos de la organización para el respaldo de información, del software y de los sistemas.

La política de respaldo debería definir los requisitos de retención y protección.

Se debería contar con instalaciones de respaldo adecuadas para garantizar que toda la información y el software esencial se pueden recuperar después de un desastre y ante una falla de los medios.

Al asignar un plan de respaldo, se deberían considerar los siguientes elementos:

a) se deberían producir registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;

b) el nivel (es decir, respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de seguridad de la información involucrada y la criticidad de la información para la operación continua de la organización;

c) los respaldos se deberían almacenar en una ubicación remota, a una distancia suficiente para evitar cualquier daño ante desastres en la ubicación principal;

d) la información de respaldo debería tener un nivel de protección física y ambiental adecuada (ver cláusula 11) de acuerdo con las normas que se aplican en la ubicación principal;

e) los medios de respaldo se deberían probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debería combinar con una prueba de los procedimientos de restauración y se debería comprobar contra la restauración según sea necesario; esto se debería combinar con una prueba de los procedimientos de restauración y se debería verificar contra el tiempo de restauración necesario. Se deberían realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos;

f) en las situaciones donde la confidencialidad es importante, se deberían proteger los respaldos mediante el cifrado.

Los procedimientos operacionales deberían monitorear la ejecución de respaldos y abordar las fallas de los respaldos programados para garantizar su integridad de acuerdo con la política de respaldos.

Se deberían probar regularmente las disposiciones de respaldos para los sistemas individuales a modo de garantizar que cumplen con los requisitos de los planes de continuidad del negocio. En el caso de los sistemas y servicios críticos, las disposiciones de respaldo deberían abarcar la información de todos los sistemas, aplicaciones y datos necesarios para recuperar al sistema completo en el caso de un desastre.

Se debería determinar el período de retención de la información esencial del negocio, considerando cualquier tipo de requisito para archivar copias que se deberían retener de manera permanente.

12.4 Registro y monitoreo

Objetivo: registrar eventos y generar evidencia.

12.4.1 Registro de eventos

Control

Se deberían producir, mantener y revisar de manera periódica los registros de eventos del usuario, las excepciones, las fallas y los eventos de seguridad de la información.

Orientación sobre la implementación

Los registros de eventos deberían incluir, cuando corresponda:

a) IDs de usuarios;

b) actividades del sistema;

c) fechas, horas y detalles de los eventos clave, es decir el inicio y la finalización de la sesión;

d) la identidad del dispositivo y su ubicación si es posible, junto con el identificador del sistema;

e) los registros de los intentos de acceso al sistema exitosos y rechazados;

f) los registros de los datos exitosos y rechazados y otros intentos de acceso a los recursos;

g) los cambios a la configuración del sistema;

h) el uso de privilegios;

i) el uso de utilidades y aplicaciones del sistema;

j) los archivos y el tipo de acceso;

k) las direcciones y protocolos de redes;

l) las alarmas que se activaron con el sistema de control de acceso;

m) la activación y la desactivación de los sistemas de protección, como los sistemas de antivirus y los sistemas de detección de intrusos;

n) los registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

El registro de eventos establece las bases para los sistemas de monitoreo automatizado que son capaces de generar informes y alertas consolidadas sobre la seguridad del sistema.

Otra información

Los registros de eventos pueden contener datos sensibles e información de identificación personal. Se deberían tomar medidas de protección adecuadas para la privacidad (ver 18.1.4).

Donde sea posible, los administradores del sistema no deberían tener permisos para borrar o desactivar los registros de sus actividades (ver 12.4.3).

12.4.2 Protección del registro de información

Control

Las instalaciones de registros y la información de registro deberían estar protegidas contra la adulteración y el acceso no autorizado.

Orientación sobre la implementación

Los controles deberían apuntar a proteger contra los cambios no autorizados para registrar información y problemas operaciones con la instalación de registros incluidos:

a) alteraciones a los tipos de mensajes que se registran;

b) archivos de registro editados o eliminados;

c) capacidad de almacenamiento de los medios de archivos de registro que exceden en tamaño, lo que resulta en su incapacidad de registrar eventos o de sobrescribir los eventos registrados anteriores.

Algunos registros de auditoría pueden ser necesarios como parte de la política de retención de registros o debido a los requisitos para recopilar y retener evidencia (ver 16.1.7).

Otra información

Los registros del sistema a menudo contienen un gran volumen de información, la mayor parte de la cual es ajena al monitoreo de seguridad de la información. Para ayudar a identificar los eventos significativos con fines de seguridad de información, se debería considerar la copia automática de los tipos de mensajes adecuados a un segundo registro o el uso de utilidades adecuadas del sistema o bien herramientas de auditoría para realizar la interrogación y la racionalización de archivos.

Se debería proteger a los registros del sistema, pues si se pueden modificar o eliminar sus datos, su existencia puede crear una falsa sensación de seguridad. Se puede utilizar el copiado en tiempo real de los registros a un sistema fuera del control de un administrador u operador del sistema para resguardar los registros.

12.4.3 Registros del administrador y del operador

Control

Las actividades del administrador y del operador del sistema se deberían registrar y los registros se deberían proteger y revisar de manera regular.

Orientación sobre la implementación

Los propietarios de cuentas de usuario con privilegios pueden manipular los registros en las instalaciones de procesamiento de información bajo su control directo y, por lo tanto, puede ser necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios con privilegios.

Otra información

Se puede utilizar un sistema de detección de intrusión que se administre fuera del control de los administradores del sistema y de la red para monitorear el cumplimiento de las actividades de administración de redes.

12.4.4 Sincronización con relojes

Control

Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad con una fuente de tiempo de referencia única.

Orientación sobre la implementación

Se deberían documentar los requisitos externos e internos para la representación, la sincronización y la precisión del tiempo. Dichos requisitos pueden ser legales, normativos, contractuales, de cumplimiento con normas o para el monitoreo interno. Se debería definir una hora de referencia estándar para utilizar dentro de la organización.

Se debería documentar e implementar el enfoque de la organización para obtener una hora de referencia de fuentes externas y la manera de sincronizar los relojes internos de manera confiable.

Otra información

Para corregir la configuración de los relojes de los computadores es importante garantizar la precisión de los registros de auditoría, que pueden ser necesarios para las investigaciones o como evidencia en casos legales o disciplinarios. Los registros de auditoría imprecisos pueden obstaculizar dichas investigaciones y dañar la credibilidad de dicha evidencia. Se puede utilizar un reloj vinculado a una transmisión de tiempo de radio de un reloj atómico nacional como el reloj maestro para los sistemas de registro. Se puede utilizar un protocolo de tiempo para mantener a todos los servidores en sincronización con el reloj maestro.

12.5 Control de software operacional

Objetivo: garantizar la integridad de los sistemas operacionales.

12.5.1 Instalación de software en sistemas operacionales

Control

Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para controlar los cambios de software en los sistemas operacionales:

a) la actualización del software operacional, las aplicaciones y las bibliotecas de programas solo la deberían realizar administradores capacitados luego de obtener la autorización correspondiente de la dirección (ver 9.4.5);

b) los sistemas operacionales solo deberían tener un código ejecutable aprobado y no un código de desarrollo o compiladores;

c) las aplicaciones y el software de sistema operativo solo se debería implementar después de realizar pruebas exhaustivas y exitosas; las pruebas deberían cubrir la capacidad de uso, la seguridad, los efectos en otros sistemas y la facilidad de uso para los usuarios en sistemas independientes (ver 12.1.4); es necesario asegurarse de que todas las bibliotecas de fuentes de programas correspondientes se han actualizado;

d) se debería utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como también la documentación del sistema;

e) debería existir una estrategia de reversión antes de que se implementen los cambios;

f) se debería mantener un registro de auditoría de todas las actualizaciones a las bibliotecas de programas operacionales;

g) se deberían retener las versiones anteriores del software de aplicación como medida de contingencia;

h) se deberían archivar las versiones antiguas de software, junto con toda la información, los parámetros, los procedimientos y los detalles de configuración necesarios que soportan al software mientras que se mantienen los datos en el archivo.

Se debería mantener el software suministrado por proveedores que se utiliza en los sistemas operacionales a un nivel al que preste soporte el operador. Con el tiempo, los proveedores de software dejarán de prestar soporte a las versiones anteriores de software. La organización debería considerar los riesgos de utilizar software sin soporte.

Cualquier decisión de actualizar a una nueva versión debería considerar los requisitos del negocio para el cambio y la seguridad de la versión, es decir, la introducción de nuevas funcionalidades de seguridad de la información o la cantidad y la gravedad de los problemas de seguridad de la versión que afectan a esta nueva versión. Se deberían aplicar parches de software cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad de información (ver 12.6).

Solo se debería dar acceso físico o lógico a los proveedores para fines de soporte cuando sea necesario y con la aprobación de la dirección. Se deberían monitorear las actividades del proveedor (ver 15.2.1).

El software informático puede utilizar software y módulos suministrados de manera externa, los que se deberían monitorear y controlar para evitar cambios no autorizados y que pueden introducir falencias en la seguridad.

12.6 Administración de vulnerabilidades técnicas

Objetivo: evitar la explotación de vulnerabilidades técnicas.

12.6.1 Administración de vulnerabilidades técnicas

Control

Se debería obtener la información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna; la exposición de la organización a dichas vulnerabilidades se debería evaluar y se deberían tomar las medidas necesarias para abordar el riesgo asociado.

Orientación sobre la implementación

Un inventario de activos actual y completo (ver cláusula 8) es un prerrequisito para la administración eficaz de vulnerabilidades técnicas. La información específica necesaria para apoyar la administración de vulnerabilidades técnicas incluye al proveedor de software, los números de versiones, el estado actual de la implementación (es decir, qué software se instala en qué sistemas) y las personas responsables del software dentro de la organización.

Se deberían tomar medidas adecuadas y oportunas en respuesta a la identificación de las posibles vulnerabilidades técnicas. Se deberían seguir los próximos puntos de orientación para establecer un proceso de administración eficaz para las vulnerabilidades técnicas:

a) la organización debería definir y establecer los roles y las responsabilidades asociadas a la administración de vulnerabilidades técnicas, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidad, los parches, el seguimientos de activos y cualquier tipo de responsabilidades de coordinación necesarias;

b) se deberían identificar los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos, ver 8.1.1); estos recursos de información se deberían actualizar en base a los cambios en el inventario o cuando se encuentran nuevos recursos útiles;

c) se debería definir una línea de tiempo para reaccionar frente a las notificaciones de vulnerabilidades técnicas posiblemente relevantes;

d) una vez que se ha identificado una vulnerabilidad técnica, la organización debería identificar los riesgos asociados y las medidas que se deberían tomar, dichas medidas podrían involucrar la aplicación de parches a los sistemas vulnerables o la aplicación de otros controles;

e) en función de la urgencia con la que se deba abordar una vulnerabilidad técnica, la medida tomada se debería realizar de acuerdo a los controles relacionados con la administración de cambios (ver 12.1.2) o siguiendo los procedimientos de respuesta ante incidentes de seguridad (ver 16.1.5);

f) si existe un parche disponible de una fuente legítima, se deberían evaluar los riesgos asociados a la instalación del parche (los riesgos que impone la vulnerabilidad se deberían comparar con el riesgo de instalar el parche);

g) los parches se pueden evaluar y probar antes de su instalación para garantizar que son eficaces y no involucran efectos colaterales que no se pueden tolerar; si no existen parches disponibles se deberían considerar otros controles como:

   1) desactivar todos los servicios o capacidades relacionadas a la vulnerabilidad;

   2) adaptar o agregar controles de acceso, es decir, firewalls, en las fronteras de la red (ver 13.1);

   3) mayor monitoreo para detectar ataques reales;

   4) concientizar sobre la vulnerabilidad;

h) se debería mantener un registro de auditoría para todos los procedimientos que se realizan;

i) el proceso de vulnerabilidad técnica se debería monitorear y evaluar regularmente para poder garantizar su efectividad y eficiencia;

j) se deberían abordar primero los sistemas en alto riesgo;

k) se debería alinear un proceso de administración de vulnerabilidades técnicas eficaz con actividades de administración de incidentes para comunicar los datos sobre vulnerabilidades con la función de respuesta ante incidentes y proporcionar los procedimientos técnicos en caso de que ocurra un incidente;

l) definir un procedimiento para abordar la situación donde se ha identificado una vulnerabilidad, pero donde no existe una contramedida. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las medidas defectivas y correctivas adecuadas.

Otra información

La administración de vulnerabilidades técnicas se puede ver como una subfunción de la administración de cambios y como tal, puede aprovechar los procesos y procedimientos de administración de cambios (ver 12.1.2 y 14.2.2).

Los proveedores a menudo se encuentran bajo gran presión para presentar nuevos parches lo más pronto posible. Por lo tanto, existe la posibilidad de que un parche no aborde el problema de manera adecuada y que presente efectos secundarios negativos. Además, en algunos casos, la desinstalación de un parche no se puede lograr fácilmente una vez que se ha aplicado un parche.

Si no es posible realizar pruebas adecuadas a los parches, es decir, por motivos de costos o falta de recursos, se puede considerar un retraso en los parches para evaluar los riesgos asociados, en base a la experiencia informada por otros usuarios. El uso de ISO/IEC 27031 puede ser beneficioso.

12.6.2 Restricciones en la instalación de software

Control

Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

Orientación sobre la implementación

La organización debería definir y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

Se debería aplicar el principio de los menores privilegios. Si se les otorgan ciertos privilegios, es posible que los usuarios tengan la capacidad de instalar software. La organización debería definir qué tipos de instalaciones de software se permiten (es decir, actualizaciones y parches de seguridad al software existente) y qué tipos de instalaciones se prohíben (es decir, software que es solo para el uso personal y software cuya categoría en cuanto a su posible característica maliciosa es desconocida o sospechosa). Estos privilegios se deberían otorgar considerando los roles de los usuarios involucrados.

Otra información

La instalación no controlada de software en dispositivos computacionales puede dar pie a la introducción de vulnerabilidades y a la fuga de información, a la falta de integridad u otros incidentes de seguridad de información o bien a la transgresión de derechos de propiedad intelectual.

12.7 Consideraciones sobre la auditoría de los sistemas de información

Objetivo: minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

12.7.1 Controles de auditoría de los sistemas de información

Control

Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales para minimizar las interrupciones a los procesos comerciales.

Orientación sobre la implementación

Se deberían observar las siguientes pautas:

a) se deberían acordar los requisitos de auditoría para el acceso a los sistemas y a los datos con la dirección correspondiente;

b) se debería acordar y controlar el alcance de las pruebas de auditoría;

c) las pruebas de auditoría se deberían limitar al acceso de solo lectura del software y los datos;

d) el acceso que no sea de solo lectura solo se debería permitir para las copias aisladas de los archivos del sistema, que se deberían borrar una vez que finaliza la auditoría o se les debería otorgar la protección adecuada si existe una obligación de mantener tales archivos de acuerdo con los requisitos de documentación de auditoría;

e) se deberían identificar y acordar los requisitos para el procesamiento especial o adicional;

f) las pruebas de auditoría que pudieran afectar la disponibilidad del sistema se deberían ejecutar fuera de las horas laborales;

g) todo el acceso se debería monitorear y registrar para producir un seguimiento de referencia.

13 Seguridad en las comunicaciones

13.1 Administración de la seguridad de redes

Objetivo: garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.

13.1.1 Controles de red

Control

Se deberían administrar y controlar las redes para proteger la información en los sistemas y aplicaciones.

Orientación sobre la implementación

Se deberían implementar controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados del acceso no autorizado. En particular, se deberían considerar los siguientes elementos:

a) se deberían establecer las responsabilidades y procedimientos para la administración de los equipos de redes;

b) se debería separar la responsabilidad operacional para la redes de las operaciones informáticas donde corresponda (ver 6.1.2);

c) se deberían establecer controles especiales para resguardar la confidencialidad y la integridad de los datos que se pasan a redes públicas o a través de redes inalámbricas y para proteger a los sistemas y aplicaciones conectados (ver cláusula 10 y 13.2); es posible que se requieran controles especiales para mantener la disponibilidad de los servicios de red y los computadores conectados;

d) se deberían aplicar los registros y monitoreos adecuados para permitir el registro y la detección de acciones que pueden afectar o que son pertinentes a la información de seguridad;

e) las actividades de administración se deberían coordinar de cerca tanto para optimizar el servicio a la organización como para garantizar que los controles se aplican de manera coherente a través de toda la infraestructura de procesamiento;

f) se deberían autenticar los sistemas de la red;

g) se debería restringir la conexión de los sistemas a la red.

Otra información

Puede encontrar información adicional sobre la seguridad de las redes en ISO/IEC 27033.

13.1.2 Seguridad de los servicios de redes

Control

Se deberían identificar e incluir en los acuerdos de servicio los mecanismos de seguridad, los niveles de servicios y los requisitos de administración de todos los servicios de redes, ya sea que estos servicios se entreguen de manera interna o se externalicen.

Orientación sobre la implementación

Se debería determinar y monitorear de manera regular la capacidad del proveedor de servicios de red para administrar los servicios de manera segura y, se debería acordar el derecho a la auditoría.

Se deberían identificar las disposiciones de seguridad necesarias para ciertos servicios, como las funciones de seguridad, los niveles de servicio y los requisitos de administración. La organización debería garantizar que los proveedores de servicios de red implementen estas medidas.

Otra información

Los servicios de red incluyen la provisión de conexiones, servicios de redes privadas y redes con valor agregado y, soluciones de seguridad de redes administradas como firewalls y sistemas de detección de intrusión. Estos servicios abarcan desde la banda ancha no administrada simple a las ofertas complejas con valor agregado.

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

a) con aplicación de tecnología para la seguridad de los servicios de redes, como la autenticación, el cifrado y los controles de conexión de redes;

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

c) los procedimientos para el uso de servicios de redes para restringir el acceso a los servicios de red o aplicaciones, donde corresponda;

13.1.3 Segregación en las redes

Control

Se deberían segregar los grupos de servicios de información, usuarios y sistemas de información en las redes.

Orientación sobre la implementación

Un método para administrar la seguridad de redes de gran tamaño es dividirlas en distintos dominios de red. Los dominios se pueden seleccionar en base a niveles de confianza (es decir, dominio de acceso público, dominio de escritorio, dominio de servidor), junto con unidades organizacionales (es decir, recursos humanos, finanzas, marketing) o alguna combinación (es decir, el dominio del servidor que se conecta a varias unidades organizacionales). La segregación se puede realizar mediante redes con diferencias físicas o mediante el uso de distintas redes lógicas (es decir, conexión de redes privadas virtuales).

Se debería definir correctamente el perímetro de cada dominio. Se permite el acceso entre dominios de red, pero se debería controlar en el perímetro mediante una puerta de enlace (es decir, firewall, enrutador de filtrado). Los criterios para la segregación de redes en los dominios y el acceso que se permite a través de las puertas de enlace se deberían basar en una evaluación de los requisitos de seguridad de cada dominio. La evaluación se debería realizar de acuerdo a la política de control de acceso (ver 9.1.1), los requisitos de acceso, el valor y la clasificación de la información procesada y también se debería considerar el costo relativo y el impacto en el rendimiento al incorporar tecnología de puerta de enlace adecuada.

Las redes inalámbricas requieren un tratamiento especial debido al perímetro de red definido deficientemente. Para los entornos sensibles, se debería tener consideración de tratar a todos los accesos inalámbricos como conexiones externas y segregar este acceso desde las redes internas hasta que el acceso haya pasado a través de una puerta de enlace de acuerdo con la política de controles de red (ver 13.1.1) antes de otorgar acceso a los sistemas internos.

Las tecnologías de autenticación, cifrado y de control de acceso a redes de nivel de usuario de las redes moderas y basadas en normas inalámbricas puede ser suficiente para dirigir la conexión a la red interna de la organización cuando se implementen adecuadamente.

Otra información

Las redes a menudo se extienden más allá de los límites organizacionales, debido a que se forman sociedades comerciales que requieren la interconexión o que comparten la información de instalaciones de redes y procesamiento de información. Tales extensiones pueden aumentar el riesgo del acceso no autorizado a los sistemas de información de la organización que utilizan la red, algunos de los cuales requieren protección de otros usuarios de red debido a su sensibilidad o criticidad.

13.2 Transferencia de información

Objetivo: mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos sobre la transferencia de información

Control

Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.

Orientación sobre la implementación

Los procedimientos y controles que se deberían seguir al utilizar instalaciones de comunicación para la transferencia de información deberían considerar los siguientes elementos:

a) procedimientos diseñados para proteger la información transferida de la intercepción, la copia, la modificación, el ruteo incorrecto y la destrucción;

b) los procedimientos para la detección y protección contra el malware que se pueden transmitir a través del uso de comunicaciones electrónicas (ver 12.2.1);

c) los procedimientos para proteger la información electrónica sensible comunicada en forma de elemento adjunto;

d) la política o las pautas que describen el uso aceptable de las instalaciones de comunicación (ver 8.1.3);

e) que el personal, las partes externas y cualquier otra responsabilidad del usuario no comprometa a la organización, es decir, a través de la difamación, el acoso, la imitación, reenvío de cartas de cadena, compra no autorizada, etc.;

f) uso de técnicas criptográficas, es decir, para proteger la confidencialidad, la integridad y la autenticidad de la información (ver cláusula 10);

g) retención y eliminación de pautas para toda la correspondencia comercial, incluidos los mensajes, de acuerdo con las normativas y a la legislación local y nacional pertinentes;

h) los controles y las restricciones asociados al uso de instalaciones de comunicación, es decir, el reenvío automático de correos electrónico a direcciones de correo externas;

i) asesorar al personal para tomar las precauciones correspondientes para no revelar información confidencial.

j) no dejar mensajes que contienen información confidencial en máquinas contestadores debido a que personas no autorizadas pueden volver a reproducir los mensajes, se pueden almacenar en sistemas comunales o almacenar incorrectamente como consecuencia de una mala manipulación;

k) informar al personal sobre los problemas del uso de máquinas o servicios de fax, a saber:

   1) el acceso no autorizado a tiendas de mensajes incorporadas para recuperar mensajes;

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

   3) envío de documentos y mensajes al número incorrecto ya sea por un error en la marcación o el uso del número almacenado incorrecto.

Además, se debería recordar al personal que no deberían sostener conversaciones confidenciales en lugares públicos o a través de canales de comunicación, oficinas abiertas y lugares de encuentro inseguros.

Los servicios de transferencia de información deberían cumplir con cualquier tipo de requisitos legales (ver 18.1).

Otra información

La transferencia de información puede ocurrir a través del uso de varios tipos distintos de instalaciones de comunicación, incluido el correo electrónico, de voz, fax y video.

La transferencia de software puede ocurrir a través de varios medios distintos, incluida la descarga de internet y la adquisición de proveedores que venden los productos listos para usar.

Se deberían considerar las implicaciones comerciales, legales y de seguridad asociada al intercambio de datos electrónico, el comercio electrónico y las comunicaciones electrónicas y los requisitos para los controles.

13.2.2 Acuerdos sobre la transferencia de información

Control

Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

Orientación sobre la implementación

Los acuerdos de transferencia de información deberían incorporar lo siguiente:

a) administración de responsabilidades para controlar y notificar la transmisión, el despacho y la recepción;

b) procedimientos para garantizar la capacidad de seguimiento y no repudiación;

c) normas técnicas mínimas para el empaque y la transmisión;

d) acuerdos de garantía en depósito;

e) normas de identificación de courier;

f) responsabilidades en caso de incidentes de seguridad de la información, como la pérdida de datos;

g) uso de un sistema de etiquetado acordado para la información sensible o crítica, que garantice que el significado de las etiquetas se comprenda inmediatamente y que la información se proteja adecuadamente (ver 8.2);

h) normas técnicas para registrar y leer la información y software;

i) cualquier control especial necesario para proteger elementos sensibles, como criptografía (ver cláusula 10);

j) mantener una cadena de custodia para la información durante el tránsito;

k) niveles aceptables de control de acceso.

Se deberían establecer y mantener políticas, procedimientos y normas para proteger la información y los medios físicos en tránsito (ver 8.3.3) y se debería hacer referencias a ellos en tales acuerdos de transferencia.

El contenido de información de seguridad de cualquier acuerdo debería 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. Para la información confidencial, los mecanismos que se utilizan para la transferencia de dicha información deberían ser coherentes para todas las organizaciones y tipos de acuerdos.

13.2.3 Mensajería electrónica

Control

Se debería proteger correctamente la información involucrada en la mensajería electrónica.

Orientación sobre la implementación

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

a) proteger a los mensajes del acceso no autorizado, de la modificación o negación de servicio de acuerdo con el esquema de clasificación adoptado por la organización;

b) garantizar la dirección y el transporte correcto del mensaje;

c) confiabilidad y disponibilidad del servicio;

d) consideraciones legales, por ejemplo, los requisitos de firmas electrónicas;

e) obtener la aprobación antes del uso de servicios públicos externos como la mensajería instantánea, las redes sociales o el compartir archivos;

f) niveles más fuertes de acceso para el control de la autenticación desde redes de acceso público.

Otra información

Existen varios tipos de mensajería electrónica como el correo electrónico, el intercambio de datos electrónico y las redes sociales, que desempeñan una función en las comunicaciones comerciales.

13.2.4 Confidencialidad de los acuerdos de no divulgación

Control

Los requisitos para los acuerdos de confidencialidad y no divulgación que reflejan las necesidades de la organización para la protección de información se deberían identificar, revisar y documentar de manera regular.

Orientación sobre la implementación

La confidencialidad de los acuerdos de no divulgación deberían abordar el requisito para proteger la información confidencial mediante términos que se pueden hacer cumplir legalmente. Los acuerdos de confidencialidad o no divulgación se aplican a las partes externas o a los empleados de la organización. Se deberían seleccionar o agregar elementos considerando el tipo de la otra parte y el acceso que se le permite o el manejo de la información confidencial. Se deberían considerar los siguientes elementos para identificar los requisitos de confidencialidad o para los acuerdos de no divulgación:

a) una definición de la información que se protegerá (es decir, información confidencial);

b) duración esperada de un acuerdo, incluidos los casos donde es posible que sea necesario mantener la confidencialidad de manera indefinida;

c) acciones necesarias al terminar un acuerdo;

d) responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada;

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

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

g) el derecho para auditar y monitorear actividades que involucran información confidencial;

h) el proceso para notificar e informar la divulgación no autorizada o la fuga de información confidencial;

i) términos para la información que se va a regresar o destruir al término del acuerdo;

j) medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo.

En base a los requisitos de seguridad de la información de la organización, es posible que se deban incluir otros elementos en un acuerdo de confidencialidad o de no divulgación.

Los acuerdos de confidencialidad y no divulgación deberían cumplir con todas las leyes y normativas pertinentes para la jurisdicción a la que corresponden (ver 18.1).

Se deberían revisar periódicamente los requisitos de los acuerdos de confidencialidad y no divulgación y cuando ocurran cambios que tengan una influencia en estos requisitos.

Otra información

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

Es posible que una organización deba utilizar distintas formas de acuerdos de confidencialidad o no divulgación en distintas circunstancias.

14 Adquisición, desarrollo y mantenimiento de sistemas

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en redes públicas.

14.1.1 Análisis y especificación de los requisitos de seguridad de la información

Control

Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas de información o en las mejoras a los sistemas de información existentes.

Orientación sobre la implementación

Los requisitos de seguridad de la información se deberían identificar utilizando diversos métodos como la derivación de requisitos de cumplimiento de políticas y normativas, modelamiento de amenazas, revisiones de incidentes o el uso de umbrales de vulnerabilidad. Se deberían documentar los resultados de la identificación y los deberían revisar todas las partes interesadas.

Los requisitos y controles de seguridad de la información reflejan el valor comercial de la información involucrada (ver 8.2) y el posible impacto negativo para el negocio que se puede generar por la falta de seguridad adecuada.

La identificación y la administración de los requisitos de seguridad de la información y los procesos asociados se deberían integrar en las primeras etapas de los proyectos de sistemas de información. Una consideración anticipada de los requisitos de seguridad de la información, es decir, en la etapa de diseño puede llevar a soluciones más eficaces y económicas.

Los requisitos de seguridad en la información también deberían considerar:

a) el nivel de confianza que se requiere en cuanto a la identidad que afirman tener los usuarios, para poder derivar los requisitos de autenticación de usuarios;

b) acceso a los procesos de provisión y autorización, para los usuarios del negocio, así como también para los usuarios con privilegios o técnicos;

c) informar a los usuarios y operadores de sus deberes y responsabilidades técnicas;

d) las necesidades de protección que requieren los activos involucrados, en particular, en cuanto a la disponibilidad, la confidencialidad y la integridad;

e) los requisitos que derivan de los procesos comerciales, como el registro y el monitoreo de transacciones, los requisitos de no repudio;

f) los requisitos impuestos por otros controles de seguridad, es decir, las interfaces al registro y monitoreo o los sistemas de detección de fugas de datos.

Para las aplicaciones que brindan servicios a través de redes públicas o que implementan transacciones, se deberían considerar los controles dedicados 14.1.2 y 14.1.3.

Si se adquieren productos, se debería seguir un proceso de pruebas y adquisiciones formal. Los contratos con el proveedor deberían abordar los requisitos de seguridad identificados.

Cuando la funcionalidad de seguridad en un producto propuesto no satisfaga el requisito específico, se deberían reconsiderar tanto el riesgo introducido como los controles asociados antes de adquirir el producto.

Se debería evaluar e implementar la orientación disponible para la configuración de seguridad del producto en línea con el software final / pila de servicio de ese sistema.

Se deberían definir los criterios para aceptar productos, es decir, en términos de su funcionalidad, lo que dará la seguridad de que se cumplen los requisitos de seguridad identificados. Se deberían evaluar los productos contra estos criterios antes de la adquisición. Se debería revisar la funcionalidad adicional para garantizar que no introduce riesgos adicionales inaceptables.

Otra información

Las normas ISO/IEC 27005 e ISO 31000 brindan orientación sobre el uso de procesos de administración de riesgos para identificar los controles para cumplir con los requisitos de seguridad de la información.

14.1.2 Protección de servicios de aplicación en redes públicas

Control

La información involucrada en los servicios de aplicación que pasan a través de redes públicas se deberían proteger contra la actividad fraudulenta, la disputa de contratos y la información y modificación no autorizada.

Orientación sobre la implementación

Las consideraciones de seguridad de la información para los servicios de aplicación que pasan a través de redes públicas deberían incluir lo siguiente:

a) el nivel de confianza que requiere cada parte sobre la identidad manifestada de la otra, es decir, a través de la autenticación;

b) procesos de autorización asociados a las personas que pudieran aprobar los contenidos de, emitir o firmar documentos de transacciones clave.

c) garantizar que todos los socios en la comunicación estén completamente informados de sus autorizaciones de la provisión o el uso del servicio;

d) determinar y cumplir con los requisitos de confidencialidad, integridad, prueba de despacho y recepción de documentos clave y el no repudio de contratos, es decir, asociados con los procesos de licitación y contratos;

e) el nivel de confianza que se requiere en la integridad de documentos clave;

f) los requisitos de protección de cualquier tipo de información confidencial;

g) la confidencialidad y la integridad de cualquier transacción de órdenes, información de pago, detalles de la dirección de envío y la confirmación de los recibos;

h) el grado de verificación adecuado para verificar la información de pago proporcionada por un cliente;

i) selección del acuerdo más adecuado de forma de pago para protegerse contra los fraudes;

j) el nivel de protección necesario para mantener la confidencialidad y la integridad de la información de la orden;

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

l) responsabilidad asociada con cualquier tipo de transacciones fraudulentas;

m) requisitos de seguros.

Muchas de las consideraciones anteriores se pueden abordar con la aplicación de controles criptográficos (ver cláusula 10), considerando el cumplimiento con los requisitos legales (ver cláusula 18 y especialmente 18.1.5 para obtener más información sobre la legislación de la criptografía).

Las disposiciones de servicio de aplicaciones entre socios se deberían respaldar con un acuerdo documentado que comprometa a ambas partes a los términos de servicios acordados, incluidos los detalles de autorización [ver letra b)] de arriba).

Se deberían considerar los requisitos de resiliencia contra ataques, los que pueden incluir los requisitos para la protección de los servidores de aplicaciones involucrados o garantizar la disponibilidad de las interconexiones de redes necesarias para entregar el servicio.

Otra información

Las aplicaciones a las que se puede acceder a través de redes públicas están sujetas a una amplia gama de amenazas relacionadas con la red, como actividades fraudulentas, disputas de contrato o divulgación de la información al público. Por lo tanto, las evaluaciones de riesgo detalladas y la selección adecuada de los controles son indispensables. Los controles necesarios a menudo incluyen métodos criptográficos para la autenticación y la protección de la transferencia de datos.

Los servicios de aplicaciones pueden utilizar métodos de autenticación seguros, es decir, utilizando criptografía de clave pública y firmas digitales (ver cláusula 10) para reducir los riesgos. Además, se pueden utilizar terceros de confianza, cuando dichos servicios sean necesarios.

14.1.3 Protección de transacciones de servicios de aplicación

Control

La información involucrada en las transacciones de servicios de aplicación se debería proteger para evitar la transmisión incompleta, el enrutamiento incorrecto, la alteración no autorizada de mensajes, la divulgación no autorizada, la duplicación no autorizada de mensajes o su reproducción.

Orientación sobre la implementación

Las consideraciones de seguridad de la información para las transacciones de servicios de aplicación deberían incluir lo siguiente:

a) el uso de firmas electrónicas por parte de cada parte involucrada en la transacción;

b) todos los aspectos de la transacción, es decir, garantizando que:

   1) que la información de autenticación secreta del usuario de todas las partes sea válida y que se verifique;

   2) la transacción permanezca como confidencial;

   3) se retenga la privacidad asociada con todas las partes involucradas;

c) la ruta de comunicaciones entre todas las partes involucradas esté cifrada;

d) los protocolos que se utilizan para comunicarse entre todas las partes involucradas estén protegidos;

e) garantizar que el almacenamiento de los detalles de la transacción se ubique detrás de cualquier entorno de acceso público, es decir, en una plataforma de almacenamiento que existe en la intranet organizacional y que no se retenga ni se exponga en un medio de almacenamiento al que se pueda acceder directamente desde internet;

f) donde se utilice una autoridad confiable (es decir, para propósitos de emitir y mantener firmas digitales o certificados digitales) la seguridad se integre en todo el proceso de administración de certificado/firma descentralizado.

Otra información

El alcance de los controles adoptados se deberían conmensurar con el nivel de riesgo asociado a cada forma de transacción de servicio de aplicación.

Es posible que las transacciones deban cumplir con requisitos legales y normativos en la jurisdicción desde donde se genera, procesa, completa o almacena la transacción.

14.2 Seguridad en los procesos de desarrollo y soporte

Objetivo: garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.

14.2.1 Política de desarrollo seguro

Control

Se deberían establecer reglas para el desarrollo de software y sistemas y, se deberían aplicar a los desarrollos dentro de la organización.

Orientación sobre la implementación

El desarrollo seguro es un requisito para generar un servicio, arquitectura, software y sistema seguro. Dentro de una política de desarrollo seguro se deberían considerar los siguientes aspectos:

a) seguridad del entorno de desarrollo;

b) orientación sobre la seguridad del ciclo de vida del desarrollo de software:

   1) seguridad en la metodología de desarrollo de software;

   2) pautas de codificación segura para cada lenguaje de programación que se utiliza;

a) requisitos de seguridad en la fase de diseño;

b) puntos de verificación de seguridad dentro de los hitos del proyecto;

c) repositorios seguros;

d) seguridad en el control de la versión;

e) conocimiento de seguridad de aplicación necesario;

f) capacidad de los desarrolladores de evitar, encontrar y solucionar la vulnerabilidad.

Se deberían utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de códigos donde es posible que no se conozcan las normas que se aplican al desarrollo o donde no sean coherentes con las buenas prácticas actuales. Se deberían considerar las normas de codificación y, donde corresponda, se debería obligar su uso. Se debería capacitar a los desarrolladores en su uso y pruebas y se debería verificar su uso mediante una revisión de códigos.

Si se externaliza el desarrollo, la organización debería obtener la garantía de que la parte externa cumple con estas reglas para el desarrollo seguro (ver 14.2.7).

Otra información

El desarrollo también se puede realizar dentro de aplicaciones como aplicaciones de oficina, programación, navegadores y bases de datos.

14.2.2 Procedimientos de control de cambios del sistema

Control

Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos de control de cambios formales.

Orientación sobre la implementación

Los procedimientos de control de cambios formales se deberían documentar para garantizar la integridad del sistema, las aplicaciones y productos, desde las primeras etapas del diseño a través de todos los esfuerzos de mantenimiento posteriores.

La introducción de nuevos sistemas y cambios importantes a los sistemas existentes debería seguir un proceso formal de documentación, especificación, pruebas, control de calidad e implementación administrada.

El proceso debería incluir una evaluación de riesgos, un análisis de los impactos de los cambios y la especificación de los controles de seguridad necesarios. Este proceso además de garantizar que no se vean comprometidos los procedimientos de seguridad y control, que los programadores de soporte cuenten con acceso solo para las partes del sistema necesarias para su trabajo y que se obtenga el acuerdo y la aprobación formal para cualquier cambio.

Donde sea factible, se deberían integrar los procedimientos de control de cambios de aplicación y operacionales (ver 12.1.2). Los procedimientos de control de cambios deberían incluir, pero sin limitarse a:

a) mantenimiento de un registro de niveles de autorización acordados;

b) garantizar que los cambios los emiten los usuarios autorizados;

c) revisar los procedimientos de control e integridad para garantizar que no se verán comprometidos por los cambios;

d) identificación de todo el software, la información, las entidades de la base de datos y el hardware que requiere modificaciones;

e) identificación y verificación del código crítico de seguridad para minimizar la probabilidad de debilidad de seguridad conocidas;

f) obtención de una aprobación formal para las propuestas detalladas antes de que comience el trabajo;

g) asegurarse de que los usuarios autorizados acepten los cambios antes de la implementación;

h) asegurarse de que la documentación establecida del sistema se actualice al finalizar cada cambio y que la documentación antigua se archive o elimine;

i) mantener un control de versión para todas las actualizaciones de software;

j) mantener un seguimiento de auditoría de todas las solicitudes de cambio;

k) asegurarse de que la documentación operativa (ver 12.1.1) y los procedimientos se cambien según sea necesario para seguir siendo adecuados;

l) asegurarse de que la implementación de cambios se realice en el momento adecuado y que no interrumpa los procesos comerciales involucrados.

Otra información

El cambio de software puede generar un impacto en el entorno operacional y viceversa.

Las buenas prácticas incluyen las pruebas de nuevo software en un entorno segregado de los entornos de producción y desarrollo (ver 12.1.4). Esto brinda una forma de tener control del nuevo software y permite una protección adicional de la información operacional que se utiliza para fines de pruebas. Esto debería incluir parches, paquetes de servicio y otras actualizaciones.

Donde se consideren actualizaciones automáticas, se debería medir el riesgo a la integridad y a la disponibilidad del sistema contra el beneficio de la implementación rápida de actualizaciones. Las actualizaciones automáticas no se deberían utilizar en sistemas críticos, pues algunas actualizaciones pueden hacer que las aplicaciones críticas fallen.

14.2.3 Revisión técnica de las aplicaciones después de los cambios en la plataforma operativa

Control

Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio se deberían revisar y probar para asegurarse de que no se ha generado un impacto adverso en las operaciones o en la seguridad de la organización.

Orientación sobre la implementación

Este proceso debería cubrir:

a) revisión de los procedimientos de control e integridad de aplicaciones para garantizar que no se verán comprometidos por los cambios en la plataforma operativa;

b) asegurarse de que se entregue una notificación de los cambios en la plataforma operativa a tiempo para permitir que se realicen las pruebas y revisiones correspondientes antes de la implementación.

c) asegurarse de que se realicen los cambios adecuados a los planes de continuidad comercial (ver cláusula 17).

Otra información

Las plataformas operativas incluyen sistemas operativos, bases de datos y plataformas middleware. El control también se debería aplicar a los cambios de aplicaciones.

14.2.4 Restricciones a los cambios de paquetes de software

Control

Se deberían desalentar las modificaciones a los paquetes de software, limitándose a los cambios necesarios y todos los cambios se deberían controlar estrictamente.

Orientación sobre la implementación

En lo posible y mientras sea factible, se deban utilizar los paquetes de software proporcionados por proveedores sin modificaciones. Cuando sea necesario modificar un paquete de software se deberían considerar los siguientes puntos:

a) el riesgo de controles integrados y los procesos de integridad comprometidos;

b) si se debería obtener el consentimiento del proveedor;

c) la posibilidad de obtener los cambios necesarios del proveedor como actualizaciones estándar de programas;

d) el impacto si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios;

e) compatibilidad con otro software en uso.

Si los cambios son necesarios se debería retener el software original y los cambios se deberían aplicar a una copia asignada. Se debería implementar un proceso de administración de actualizaciones para garantizar que se instalan los parches aprobados más recientes y las actualizaciones de aplicaciones para todo el software autorizado (ver 12.6.1). Todos los cambios se deberían probar y documentar completamente, de modo que se puedan volver a aplicar, en caso de ser necesario, a futuras actualizaciones de software. En caso de ser necesario las modificaciones de deberían probar y validar con una entidad de evaluación independiente.

14.2.5 Principios de ingeniería segura del sistema

Control

Se deberían establecer, documentar, mantener y aplicar los principios para la ingeniería de sistemas seguros para cualquier labor de implementación del sistema de información.

Orientación sobre la implementación

Se deberían establecer, documentar y aplicar los procedimientos de ingeniería de sistemas de información segura en base a los principios de ingeniería de seguridad a las actividades de ingeniería del sistema de información interno. La seguridad se debería diseñar en todos los niveles de la arquitectura (negocios, datos, aplicaciones y tecnología) equilibrando la necesidad de la seguridad de la información con la necesidad de la accesibilidad. Se debería analizar la tecnología nueva para conocer sus riesgos de seguridad y el diseño se debería revisar contra los patrones de ataque conocidos.

Estos principios y los procedimientos de ingeniería establecidos se deberían revisar de manera regular para asegurarse de que contribuyen de manera eficaz a las normas de seguridad mejoradas dentro del proceso de ingeniería.

También se deberían revisar de manera regular para asegurarse de que permanecen vigentes en cuanto al combate contra cualquier posible amenaza y que sigan siendo aplicables a los avances de las tecnologías y soluciones que se están aplicando.

Se deberían aplicar los principios de ingeniería de seguridad establecidos, donde corresponda, a los sistemas de información externalizados a través de contratos y otros acuerdos vinculantes entre la organización y el proveedor a quien la organización externaliza el servicio. La organización debería confirmar que el rigor de los principios de ingeniería de seguridad del proveedor es comparable con el propio.

Otra información

Los procedimientos de desarrollo de aplicaciones deberían aplicar técnicas de ingeniería seguras en el desarrollo de aplicaciones que tienen interfaces de entrada y salida. Las técnicas de ingeniería segura brindan orientación sobre las técnicas de autenticación de usuario, control y validación de datos de sesión seguros, sanitización y eliminación de códigos de depuración.

14.2.6 Entorno de desarrollo seguro

Control

Las organizaciones deberían establecer y proteger adecuadamente a los entornos de desarrollo seguros para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

Orientación sobre la implementación

Un entorno de desarrollo seguro incluye a las personas, procesos y tecnologías asociadas con el desarrollo e integración de sistemas.

Las organizaciones deberían evaluar los riesgos asociados con las labores de desarrollo de sistemas individuales y establecer entornos de desarrollo seguro para labores de desarrollo del sistema específicas, considerando:

a) la sensibilidad de los datos que el sistema procesará, almacenará y transmitirá;

b) los requisitos externos e internos correspondientes, es decir, de las normativas o políticas;

c) controles de seguridad que ya ha implementado la organización y que soportan el desarrollo del sistema;

d) confiabilidad del personal que trabaja en el entorno (ver 7.1.1);

e) el grado de externalización asociado al desarrollo del sistema;

f) la necesidad de contar con segregación entre distintos entornos de desarrollo;

g) control del acceso al entorno de desarrollo;

h) monitoreo del cambio al entorno y al código que ahí se almacena;

i) que los respaldos se almacenen en ubicaciones fuera del sitio;

j) control sobre el movimiento de datos desde y hacia el entorno.

Una vez que se ha determinado el nivel de protección para un entorno de desarrollo específico, las organizaciones deberían documentar los procesos correspondientes en los procedimientos de desarrollo seguro y proporcionarlos a todas las personas que los necesiten.

14.2.7 Desarrollo externalizado

Control

La organización debería supervisar y monitorear la actividad del desarrollo externalizado del sistema.

Orientación sobre la implementación

Donde se externalice el desarrollo del sistema, se deberían considerar los siguientes puntos en toda la cadena de suministro de la organización:

a) disposiciones de licenciamiento, derechos de propiedad de código y de propiedad intelectual relacionados al contenido externalizado (ver 18.1.2);

b) los requisitos contractuales para el diseño, la codificación y las prácticas de pruebas seguras (ver 14.2.1);

c) provisión del modelo de amenazas aprobado para el desarrollador externo;

d) prueba de aceptación de la calidad y precisión de los entregables;

e) provisión de evidencia de que se utilizaron umbrales de seguridad para establecer niveles aceptables mínimos de seguridad y calidad de la privacidad;

f) provisión de evidencia de que se ha aplicado una cantidad suficiente de pruebas para protegerse contra la ausencia intencional y no intencional de contenido malicioso después de la entrega;

g) provisión de evidencia de que se han aplicado pruebas suficientes para protegerse contra la presencia de vulnerabilidades conocidas;

h) disposiciones de garantía en depósito, es decir, que el código de fuente ya no está disponible;

i) el derecho contractual para auditar procesos y controles de desarrollo;

j) documentación eficaz sobre el entorno de desarrollo utilizado para crear los entregables;

k) la organización sigue siendo responsable del cumplimiento con las leyes pertinentes y la verificación de la eficiencia del control.

Otra información

Puede encontrar información adicional sobre las relaciones con proveedores en ISO/IEC 27036.

14.2.8 Pruebas de seguridad del sistema

Control

Las pruebas de la funcionalidad de seguridad se deberían realizar durante el desarrollo.

Orientación sobre la implementación

Los sistemas nuevos y actualizados se deberían someter a pruebas y verificaciones exhaustivas durante los procesos de desarrollo, incluida la preparación de un programa de actividades detallado y entradas de pruebas y los resultados esperados bajo una variedad de condiciones. Para los desarrollos internos, dichas pruebas las debería realizar inicialmente el equipo de desarrollo. Las pruebas de aceptación independientes se deberían realizar (tanto para los desarrollos internos y externalizados) para garantizar que el sistema funciona según se espera y solo como se espera (ver 14.1.1 y 14.1.9). El alcance de las pruebas debería ser en proporción a la importancia y naturaleza del sistema.

14.2.9 Pruebas de aceptación del sistema

Control

Se deberían establecer programas de pruebas de aceptación y criterios relacionados para los nuevos sistemas de información, actualizaciones y nuevas versiones.

Orientación sobre la implementación

Las pruebas de aceptación del sistema deberían incluir las pruebas de los requisitos de seguridad de la información (ver 14.1.1 y 14.1.2) y la adherencia a las prácticas de desarrollo del sistema seguro (ver 14.2.1). Las pruebas también se deberían realizar en los componentes y sistemas integrados recibidos. Las organizaciones pueden aprovechar las herramientas automatizadas, como las herramientas de análisis de códigos o los escáneres de vulnerabilidad y debería verificar la remediación de los defectos relacionados con la seguridad.

Las pruebas se deberían realizar en un entorno de pruebas realista para garantizar que el sistema no introducirá vulnerabilidades al entorno de la organización y que las pruebas sean confiables.

14.3 Datos de pruebas

Objetivo: garantizar la protección de los datos que se utilizan para las pruebas.

14.3.1 Protección de los datos de pruebas

Control

Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

Orientación sobre la implementación

Se debería evitar el uso de los datos operacionales que contienen información personal identificable o cualquier otro tipo de información confidencial para fines de prueba. Si se utiliza información personal identificable o de lo contrario, información confidencial para fines de prueba, todos los detalles y contenido sensible se debería proteger mediante su retiro y modificación (ver ISO/IEC 29101).

Se deberían aplicar las siguientes pautas para proteger los datos operacionales, cuando se utilizan con fines de pruebas:

a) los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacional, también se deberían aplicar a los sistemas de aplicación de pruebas;

b) debería existir una autorización independiente cada vez que se copia la información operacional a un entorno de prueba;

c) la información operacional se debería borrar de un entorno de pruebas inmediatamente una vez que haya finalizado la prueba;

d) se debería registrar la copia y el uso de la información operacional para proporcionar un seguimiento de auditoría.

Otra información

Las pruebas del sistema y de aceptación generalmente requieren volúmenes sustanciales de datos de prueba que están lo más cercanos posibles a los datos operacionales.

15 Relaciones con los proveedores

15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: garantizar la protección de los activos de la organización accesibles a los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con los proveedores

Control

Se deberían acordar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización con el proveedor y se deberían documentar debidamente.

Orientación sobre la implementación

La organización debería identificar e imponer controles de seguridad de la información para abordar específicamente el acceso de los proveedores a la información de la organización en una política. Estos controles deberían abordar los procesos y procedimientos que implementará la organización, así como también aquellos procesos y procedimientos que la organización debería requerirle al proveedor que implemente, incluido:

a) la identificación y la documentación de los tipos de proveedores, es decir, los servicios de TI, las utilidades de logística, los servicios financieros, los componentes de la infraestructura de TI y a quiénes autorizará la organización para acceder a su información;

b) un proceso y ciclo de vida estandarizado para administrar las relaciones con los proveedores;

c) la definición de los tipos de acceso a la información que se les permitirá a los distintos tipos de proveedores y el monitoreo y control del acceso;

d) requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso para servir de base para los acuerdos individuales con los proveedores en base a las necesidades comerciales de la organización y los requisitos y su perfil de riesgo;

e) procesos y procedimientos para monitorear la adherencia a los requisitos de seguridad de información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación de productos;

f) controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes;

g) tipos de obligaciones aplicables a los proveedores para proteger la información de la información;

h) manejo de incidentes y contingencias asociadas con el acceso a los proveedores, incluidas las responsabilidades de la organización y los proveedores;

i) resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;

j) capacitación de concientización para el personal de la organización involucrado en las adquisiciones sobre políticas, procesos y procedimientos correspondientes;

k) capacitación de concientización para el personal de la organización que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización;

l) las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;

m) administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.

Otra información

La información no se puede poner en riesgo por los proveedores con una administración de seguridad de información inadecuada. Se deberían identificar y aplicar controles para administrar el acceso de los proveedores a las instalaciones de procesamiento de la información. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se pueden utilizar acuerdos de no divulgación. Otro ejemplo son los riesgos de protección de datos cuando el acuerdo del proveedor involucra la transferencia de o el acceso a la información a través de las fronteras. La organización debería estar en conocimiento de que la responsabilidad legal o contractual para proteger a la información permanece con la organización.

15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores

Control

Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.

Orientación sobre la implementación

Se deberían establecer y documentar acuerdos con los proveedores para garantizar que no existen malos entendidos entre la organización y el proveedor en cuanto a las obligaciones de ambas partes para cumplir con los requisitos de seguridad de la información pertinentes.

Se deberían considerar los siguientes términos para incluir en los acuerdos y poder satisfacer los requisitos de seguridad de la información identificados:

a) descripción de la información que se debería proporcionar o a la que se debería acceder y los métodos para proporcionar o acceder a la información;

b) clasificación de la información de acuerdo al esquema de clasificación de la organización (ver 8.2); y si es necesario también realizar el mapeo entre el esquema propio de la organización y el esquema de clasificación del proveedor;

c) requisitos legales y normativos, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor y una descripción de sobre cómo se garantizará si se cumplen;

d) obligación de cada parte contractual de implementar un conjunto de controles acordados incluido el control de acceso, la revisión de desempeño, el monitoreo, los informes y la auditoría;

e) reglas de uso aceptable de la información, incluido en uso inaceptable en caso de ser necesario;

f) una lista explícita del personal autorizado para acceder a o recibir la información o los procedimientos o condiciones de la organización para su autorización y el retiro de la autorización, para el acceso a o la recepción de la información de la organización al personal del proveedor;

g) políticas de seguridad de la información pertinentes al contrato específico;

h) requisitos y procedimientos de la administración de incidentes (en especial la notificación y la colaboración durante la remediación de incidentes);

i) requisitos de capacitación y concientización para procedimientos específicos y requisitos de seguridad de la información, es decir, para la respuesta ante incidentes y procedimientos de autorización;

j) normativas pertinentes para la subcontratación, incluidos los controles que se deberían implementar;

k) socios de acuerdos pertinentes, incluida una persona de contacto para los asuntos de seguridad de la información;

l) requisitos de selección, si existe alguno, para el personal del proveedor para realizar los procedimientos de selección y notificación si no se ha completado la selección o si los resultados dan pie a dudas o inquietudes;

m) derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo;

n) procesos de resolución de defectos y resolución de conflictos;

o) obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe;

p) obligaciones del proveedor para cumplir con los requisitos de seguridad de la organización.

Otra información

Los acuerdos pueden variar considerablemente para las distintas organizaciones y entre los distintos tipos de proveedores. Por lo tanto, se debería tener cuidado de incluir a todos los riesgos y requisitos de seguridad de la información pertinentes. Los acuerdos del proveedor también pueden involucrar a otras partes (es decir, sub-proveedores).

Los procedimientos para continuar el procesamiento en el caso de que el proveedor no pueda suministrar sus productos o servicios se deberían considerar en el acuerdo para evitar cualquier tipo de retraso en la disposición de los productos y servicios de reemplazo.

15.1.3 Cadena de suministro de la tecnología de información y comunicación

Control

Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

Orientación sobre la implementación

Se deberían considerar los siguientes temas para incluirlos en los acuerdos con el proveedor sobre la seguridad de la cadena de suministro:

a) definir los requisitos de seguridad de la información que se aplicarán a la adquisición de tecnologías, productos o servicios de información y comunicación además de los requisitos de seguridad de la información para las relaciones con el proveedor;

b) para los servicios de tecnología de información y comunicación, que requieren que los usuarios propaguen los requisitos de seguridad de la organización en toda la cadena de suministro si los proveedores realizan subcontrataciones para partes del servicio de tecnología de información y comunicación proporcionados a la organización;

c) para los productos de tecnología de información y comunicación que requieren que los proveedores propaguen las prácticas de seguridad correspondientes a través de toda la cadena de suministro si estos productos incluyen componentes comprados a otros proveedores;

d) implementación de un proceso de monitoreo y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación se adhieren a los requisitos de seguridad establecidos;

e) implementación de un proceso para identificar los componentes de los productos o servicios que son fundamentales para mantener la funcionalidad y que, por lo tanto, requiere una mayor atención y escrutinio cuando se desarrollan fuera de la organización, especialmente si el proveedor del nivel superior externalice los aspectos de los componentes de productos o servicios a otros proveedores;

f) obtención de una garantía de que los componentes críticos y su origen se pueden rastrear en toda la cadena de suministrar;

g) obtener la garantía de que los productos de tecnología de información y comunicación entregados funcionan según lo esperado sin ninguna función inesperada o no deseada;

h) definición de las reglas para compartir la información en cuanto a la cadena de suministro y cualquier posible problema y compromiso entre la organización y los proveedores;

i) implementación de procesos específicos para administrar el ciclo de vida de los componentes de tecnología de información y comunicación junto con la disponibilidad y los riesgos de seguridad asociados. Esto incluye los riesgos de los componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o a que ya no proporcionan estos componentes debido a los avances de la tecnología.

Otra información

Las prácticas de administración de riesgos de la cadena de suministro de la tecnología de información y comunicación específicas se desarrollan sobre la seguridad de la información general, la calidad, la administración de proyectos y las prácticas de ingeniería del sistema, pero no las reemplazan.

Se aconseja a las organizaciones a trabajar con los proveedores para comprender la cadena de suministro de la tecnología de información y comunicación y cualquier otro asunto que tenga un impacto importante en los productos y servicios que se proporcionan. Las organizaciones pueden influenciar las prácticas de seguridad de información de la cadena de suministro de la tecnología de información y comunicación aclarando en los acuerdos con sus proveedores los asuntos que deberían abordar proveedores en la cadena de suministro de tecnología de información y comunicación.

La cadena de suministro de tecnología de información y comunicación según se aborda aquí incluye los servicios de computación en nube.

15.2 Administración de prestación de servicios de proveedores

Objetivo: mantener un nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos del proveedor.

15.2.1 Monitoreo y revisión de los servicios del proveedor

Control

Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor de manera regular.

Orientación sobre la implementación

El monitoreo y revisión de los servicios del proveedor debería garantizar que los términos y condiciones de seguridad de la información de los acuerdos se respeten y que los incidentes y los problemas de seguridad de la información se gestionen correctamente.

Esto debería involucrar un proceso de relación administrativa de servicios entre la organización y el proveedor para:

a) monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos;

b) revisar los informes de servicio producidos por el proveedor y organizar reuniones de avance de manera regular según lo requieren los acuerdos;

c) realizar auditorías de los proveedores, en conjunto con la revisión de informes de auditores independientes, en caso de estar disponibles y, un seguimiento de los problemas identificados;

d) proporcionar información sobre los incidentes de seguridad y revisar esta información según sea necesario conforme a los acuerdos y a cualquier pauta o procedimiento de apoyo;

e) revisar los seguimientos de auditoría del proveedor y los registros de eventos de seguridad de la información, los problemas operacionales, seguimiento de todas las fallas e interrupciones relacionadas con el servicio entregado;

f) resolver y gestionar cualquier problema identificado;

g) revisar los aspectos de seguridad de la información de las relaciones que tiene el proveedor con sus propios proveedores;

h) asegurarse de que el proveedor mantiene una capacidad de servicio suficiente junto con planes de trabajo diseñados para garantizar que se mantienen los niveles de continuidad en el servicio luego de grandes fallas o desastres en el servicio (ver cláusula 17).

La responsabilidad de administrar las relaciones del proveedor se deberían asignar a una persona o equipo de administración de servicios asignado. Además, la organización se debería asegurar de que los proveedores asignen responsabilidades para revisar el cumplimiento y hacer cumplir los requisitos de los acuerdos. Se deberían tener las habilidades y recursos técnicos suficientes a disponibles para monitorear que se cumplen los requisitos del acuerdo, en particular los requisitos de seguridad de la información. Se deberían tomar las medidas necesarias cuando se observan deficiencias en la prestación de servicios.

La organización debería retener el control y la visibilidad suficientes en todos los aspectos de seguridad para la información o las instalaciones de procesamiento de información sensible o crítica que evalúa, procesa o administra un proveedor. La organización debería retener la visibilidad en las actividades de seguridad como la administración del cambio, la identificación de vulnerabilidades y los informes y respuestas ante un incidente de seguridad de información a través de un proceso de informes definido.

15.2.2 Administración de cambios en los servicios del proveedor

Control

Se deberían administrar los cambios a la provisión de servicios de parte de los proveedores, manteniendo y mejorando las políticas de seguridad de la información, los procedimientos y controles específicos, considerando la criticidad de la información comercial, los sistemas y procesos involucrados y la reevaluación de riesgos.

Orientación sobre la implementación

Se deberían considerar los siguientes aspectos:

a) cambios a los acuerdos del proveedor;

b) los cambios realizados por la organización por implementar:

   1) mejoras a los servicios que se ofrecen actualmente;

   2) desarrollo de cualquier nueva aplicación y sistemas

   3) las modificaciones o actualizaciones de las políticas y procedimientos de la organización;

   4) controles nuevos o cambiados para resolver incidentes de seguridad de la información y mejorar la seguridad;

c) cambios en los servicios del proveedor a implementarse;

   1) cambios y mejoras en las redes;

   2) uso de nuevas tecnologías;

   3) adopción de nuevos productos o nuevas versiones;

   4) nuevas herramientas y entornos de desarrollo;

   5) cambios en la ubicación física de las instalaciones de servicios;

   6) cambio de proveedores;

   7) subcontratación a otro proveedor.

16 Administración de incidentes de seguridad de la información

16.1 Administración de incidentes y mejoras de seguridad en la información

Objetivo: garantizar un enfoque coherente y eficaz a la administración de incidentes de seguridad de la información, incluida la comunicación sobre los eventos y las debilidades de seguridad.

16.1.1 Responsabilidades y procedimientos

Control

Se deberían establecer las responsabilidades y procedimientos de la dirección para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para las responsabilidades de la dirección y los procedimientos respecto de la administración de incidentes de seguridad de la información.

a) las responsabilidades de la dirección se deberían establecer para garantizar que se desarrollan y comunican los siguientes procedimientos adecuadamente dentro de la organización.

   1) procedimientos para la planificación y preparación de la respuesta ante incidentes;

   2) procedimientos para monitorear, detectar, analizar e informar sobre eventos e incidentes de seguridad;

   3) procedimientos para registrar actividades de administración de incidentes;

4) procedimientos para administrar evidencia forense;

5) procedimientos para la evaluación y la decisión sobre los eventos de seguridad de la información y la evaluación de las debilidades en la seguridad de la información;

6) procedimientos para la respuesta incluidos aquellos para el escalamiento, la recuperación controlada desde un incidente y la comunicación a las personas internas y externas u organizaciones;

b) los procedimientos establecidos deberían garantizar que:

1) el personal competente maneje los problemas relacionados a los incidentes de seguridad de la información dentro de la organización;

2) que se implemente un punto de contacto para la detección e informe de los incidentes de seguridad.

3) que se mantengan los contactos correspondientes con las autoridades, grupos de interés externos o foros que manejen los problemas relacionados con los incidentes de seguridad de la información;

c) el informe de procedimientos debería incluir:

1) la preparación de formularios de informes de eventos de seguridad de la información para apoyar la acción del informe y ayudar a la persona que lo hace a recordar todas las actividades necesarias en caso de un evento de seguridad de la información;

2) el procedimiento que se debería realizar en caso de un evento de seguridad de la información, es decir, indicando todos los detalles inmediatamente, como el tipo de incumplimiento, si ocurre una falla, los mensajes en la pantalla e informar inmediatamente al punto de contacto y realizar solo acciones coordinadas;

3) referencia a un proceso disciplinario formal establecido para lidiar con los empleados que caen en incumplimientos de seguridad;

4) procesos de retroalimentación adecuados para asegurarse de que a aquellas personas que informan eventos de seguridad se les notifique sobre los resultados una vez que se ha abordado el problema y se haya cerrado.

Los objetivos para la administración de incidentes de seguridad se deberían acordar con la dirección y se debería garantizar que las personas responsables de la administración de incidentes de seguridad de la información comprendan las prioridades de la organización para manejar incidentes de seguridad de la información.

Otra información

Los incidentes de seguridad de la información pueden trascender los límites organizacionales y nacionales. Para responder a dichos incidentes existe una necesidad en aumento para coordinar la respuesta y compartir información sobre estos incidentes con organizaciones existentes según sea pertinente.

Se proporciona orientación detallada en la administración de incidentes de seguridad en ISO/IEC 27035.

16.1.2 Informe de eventos de seguridad de la información

Control

Los eventos de seguridad de la información se deberían informar a través de canales de administración adecuados lo más pronto posible.

Orientación sobre la implementación

Todos los empleados y contratistas deberían estar en conocimiento de su responsabilidad para informar los eventos de seguridad de la información lo más pronto posible. También deberían estar en conocimiento del procedimiento para informar eventos de seguridad de la información y el punto de contacto al que se debería informar los eventos.

Las situaciones que se deberían considerar para el informe de eventos de seguridad incluyen:

a) control de seguridad ineficaz;

b) incumplimiento de la integridad, la confidencialidad o las expectativas de disponibilidad de la información;

c) errores humanos;

d) incumplimientos con las políticas o pautas;

e) incumplimientos en las disposiciones de seguridad física;

f) cambios no controlados en el sistema;

g) fallas en el software o hardware;

h) violaciones de acceso.

Otra información

Las fallas u otro comportamiento anómalo del sistema puede ser un indicador de un ataque de seguridad o un incumplimiento real de seguridad y, por lo tanto, siempre se debería informar como un evento de seguridad de la información.

16.1.3 Informe de las debilidades de la seguridad de la información

Control

Se debería requerir a los empleados y contratistas que utilizan los sistemas y servicios de información de la organización anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios.

Orientación sobre la implementación

Todos los empleados y contratistas deberían informar estos asuntos al punto de contacto lo más rápido posible para poder evitar los incidentes de seguridad de la información. El mecanismo de informes debería ser fácil, accesible y estar disponible según sea posible,

Otra información

Se debería indicar a los empleados y contratistas que no intenten indagar en debilidades de seguridad sospechosas. La prueba de debilidades se puede interpretar como un posible uso indebido del sistema y también podría provocar daños al sistema o servicio de información y generar una responsabilidad legal para la persona que realiza la prueba.

16.1.4 Evaluación de y decisión sobre los eventos de seguridad de la información

Control

Se deberían evaluar los eventos de seguridad de la información y se debería decidir si se clasificarán como incidentes de seguridad de la información.

Orientación sobre la implementación

El punto de contacto debería evaluar cada evento de seguridad de la información utilizando la escala de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento se debería clasificar como un incidente de seguridad de la información. La clasificación y la priorización de incidentes pueden ayudar a identificar el impacto y el alcance de un incidente.

En los casos donde la organización tenga un equipo de respuesta ante incidentes de seguridad (ISIRT, por sus siglas en inglés), la evaluación y la decisión se puede enviar al ISIRT para su confirmación o reevaluación.

Se deberían registrar los resultados de la evaluación y la decisión en detalle con fines de referencia y verificación futuros.

16.1.5 Respuesta ante incidentes de seguridad de la información

Control

Se debería responder ante los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.

Orientación sobre la implementación

Un punto de contacto y otras personas pertinentes de la organización o partes externas deberían responder ante los incidentes de seguridad de la información (ver 16.1.1).

La respuesta debería incluir lo siguiente:

a) recopilar la evidencia lo más pronto posible después de la ocurrencia;

b) realizar análisis forenses de seguridad de la información, según sea necesario (ver 16.1.7);

c) escalamiento, según sea necesario;

d) asegurarse de que todas las actividades de respuesta se registren correctamente para el posterior análisis;

e) comunicación de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a otras personas u organizaciones internas o externas con una necesidad de saber;

f) manejar las debilidades de la seguridad de la información que causan o contribuyen al incidente;

g) una vez que se ha manejado el incidente correctamente, se debería cerrar y registrar formalmente.

Se debería realizar un análisis post-incidente, según sea necesario, para identificar el origen del incidente.

Otra información

El primer objetivo de la respuesta ante incidentes es reanudar el “nivel de seguridad normal” y luego iniciar la recuperación necesaria.

16.1.6 Aprendizaje de los incidentes de seguridad de la información

Control

Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.

Orientación sobre la implementación

Deberían existir mecanismos para permitir los tipos, los volúmenes y los costos de los incidentes de seguridad de la información que se van a cuantificar y monitorear. Se debería utilizar la información obtenida de la evaluación de los incidentes de seguridad de la información para identificar los incidentes recurrentes o de alto impacto.

Otra información

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de contar con controles mejorados o adicionales para limitar la frecuencia, el daño y el costo de las ocurrencias futuras o bien se deberían considerar en el proceso de revisión de políticas de seguridad (ver 5.1.2).

Con el debido cuidado de los aspectos de confidencialidad, se pueden utilizar las anécdotas de los incidentes reales de información de la seguridad en la capacitación de concientización a los usuarios (ver 7.2.2) como ejemplos que pueden suceder, cómo responder a dichos incidentes y cómo evitarlos en el futuro.

16.1.7 Recopilación de evidencia

Control

La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

Orientación sobre la implementación

Se deberían desarrollar procedimientos internos y se deberían seguir al tratar con evidencia para propósitos de acciones legales y disciplinarias.

En general, estos procedimientos para la evidencia deberían proporcionar procesos para la identificación, recopilación, adquisición y preservación de evidencia de acuerdo a los distintos tipos de medios, dispositivos y estado de los dispositivos, es decir, encendidos o apagados. Los procedimientos deberían considerar:

a) cadena de custodia;

b) seguridad de la evidencia;

c) seguridad del personal;

d) roles y responsabilidades del personal involucrado;

e) competencia del personal;

f) documentación;

g) sesión informativa.

Donde corresponda, se deberían buscar certificaciones u otros medios de calificación del personal y herramientas pertinentes, para reforzar el valor de la evidencia preservada;

La evidencia forense puede trascender los límites organizacionales o jurisdiccionales. En tales casos, se debería garantizar que la organización tenga el derecho a recopilar la información necesaria como evidencia forense. También se deberían considerar los requisitos de distintas jurisdicciones para maximizar las probabilidades de admisión en las jurisdicciones pertinentes.

Otra información

La identificación es el proceso de involucrar la búsqueda de, el reconocimiento y la documentación de la posible evidencia. La recopilación es el proceso de reunir los elementos físicos que pueden contener posibles evidencias. La adquisición es el proceso de creación de una copia de datos dentro de un conjunto definido. La preservación es el proceso para mantener y resguardar la integridad y la condición original de la posible evidencia.

Cuando se detecta un evento de seguridad de la información por primera vez, puede no resultar obvio si el evento resultará o no en una acción de tribunales. Por lo tanto, existe el peligro de que se destruya la evidencia necesaria de manera intencional o accidental antes de que se reconozca la gravedad del incidente. Resulta aconsejable involucrar a un abogado o a la policía al comienzo de cualquier acción legal contemplada y recibir asesoría sobre la evidencia necesaria.

La norma ISO/IEC 27037 brinda orientación para la identificación, la recopilación, la adquisición y la preservación de evidencia digital.

17 Aspectos de la seguridad de la información de la administración de la continuidad comercial

17.1 Continuidad de la seguridad de la información

Objetivo: la continuidad de la seguridad de la información se debería integrar en los sistemas de administración de continuidad comercial.

17.1.1 Planificación de la continuidad de la seguridad en la información

Control

La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis o desastre.

Orientación sobre la implementación

Una organización debería determinar si la continuidad de la seguridad de la información se incluye dentro del proceso de administración de continuidad del negocio o dentro del proceso de administración de recuperación ante desastres. Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad comercial y la recuperación ante desastres.

En la ausencia de una continuidad comercial formal y una planificación de recuperación ante desastres, la administración de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos ante situaciones adversas, en comparación con las condiciones operacionales normales. De manera alternativa, una organización puede desarrollar un análisis de impacto comercial para los aspectos de seguridad de la información y determinar los requisitos de seguridad de la información que se aplican a situaciones adversas.

Otra información

Para poder reducir el tiempo y el esfuerzo de un análisis de impacto comercial “adicional” para la seguridad de la información, se recomienda capturar los aspectos de seguridad de la información dentro de la administración de la continuidad comercial normal o el análisis de impacto en el negocio de la administración de recuperación ante desastres. Esto implica que los requisitos de continuidad de la seguridad de la información se formulan explícitamente en la administración de la continuidad del negocio o en los procesos de administración de recuperación ante desastres.

Puede encontrar información sobre la administración de continuidad comercial en ISO/IEC 27031, ISO 22313 e ISO 22301.

17.1.2 Implementación de la continuidad de la seguridad de la información

Control

La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante situaciones adversas.

Orientación sobre la implementación

Una organización se debería asegurar de lo siguiente:

a) exista una estructura de administración adecuada para prepararse para, mitigar y responder ante un evento disruptivo que utiliza personal con la autoridad, la experiencia y la competencia necesaria;

b) se nomine al personal de respuesta ante incidentes con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información;

c) que se desarrollen y aprueben planes documentados, los procedimientos de respuesta y recuperación detallando cómo la organización administrará un evento disruptivo y mantendrá la seguridad de su información a un nivel predeterminado, en base a los objetivos de continuidad de la seguridad de la información aprobada por la dirección (ver 17.1.1).

De acuerdo a los requisitos de continuidad de la seguridad de la información, la organización debería establecer, documentar, implementar y mantener:

a) controles de seguridad de la información dentro de la continuidad comercial o los procesos, procedimientos y sistemas y herramientas de apoyo;

b) procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa;

c) controles de compensación para los controles de seguridad de la información que no se pueden mantener durante una situación adversa.

Otra información

Es posible que se hayan establecido procesos y procedimientos específicos dentro del contexto de la continuidad comercial o de la recuperación ante desastres. Se debería proteger la información que se maneja dentro de estos procesos y procedimientos o dentro de los sistemas de información dedicados para apoyarlos. Por lo tanto, una organización debería:

Involucrar a especialistas de seguridad de la información al establecer, implementar y mantener la continuidad comercial o los procesos y procedimientos de recuperación ante desastres.

Los controles de seguridad de la información que se han implementado deberían seguir funcionando durante una situación adversa. Si los controles de seguridad no pueden continuar resguardando la información, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información

Control

La organización debería verificar los controles de continuidad de seguridad de la información establecidos e implementados en intervalos regulares y poder asegurar que son válidos y eficaces durante situaciones adversas.

Orientación sobre la implementación

Los cambios organizacionales, técnicos de procedimientos y procesos, ya sean en un contexto operacional o de continuidad, pueden dar pie a cambios en los requisitos de continuidad de la seguridad de la información. En tales casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información se deberían revisar contra estos requisitos cambiados.

Las organizaciones deberían verificar la continuidad de la administración de la seguridad de la información de la siguiente forma:

a) el ejercicio y las pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que son coherentes con los objetivos de continuidad de la seguridad de la información;

b) el ejercicio y las pruebas del conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que su desempeño es coherentes con los objetivos de continuidad de la seguridad de la información;

c) revisión de la validez y la efectividad de las medidas de continuidad de la seguridad de la información cuando cambian los sistemas de información, los procesos, los procedimientos y los controles de seguridad de la información, o los procesos y soluciones de administración de administración de continuidad comercial/recuperación ante desastres.

Otra información

La verificación de los controles de continuidad de la seguridad de la información es distinta de las pruebas y verificación de seguridad de la información y se debería realizar fuera de las pruebas de los cambios. Si es posible, resulta preferible integrar la verificación de los controles de continuidad de la seguridad de la información con la continuidad comercial de la organización o las pruebas de recuperación ante desastres.

17.2 Redundancias

Objetivo: garantizar la disponibilidad de las instalaciones de procesamiento de información.

17.2.1 Disponibilidad de las instalaciones de procesamiento de la información

Control

Las instalaciones de procesamiento de la información se deberían implementar con la suficiente redundancia para cumplir con los requisitos de disponibilidad.

Orientación sobre la implementación

Las organizaciones deberían identificar los requisitos comerciales para la disponibilidad de los sistemas de información. Cuando no se pueda garantizar la disponibilidad a través de la arquitectura de sistemas existente, se deberían considerar los componentes o arquitecturas redundantes.

Donde corresponda, se deberían probar los sistemas de información redundantes para garantizar que la conmutación por error de un componente a otro funcione adecuadamente.

Otra información

La implementación de redundancias puede introducir riesgos a la integridad o a la confidencialidad de la información y los sistemas de información que se deberían considerar al diseñar los sistemas de información.

18 Cumplimiento

18.1 Cumplimiento con los requisitos legales y contractuales

Objetivo: evitar incumplimientos a las obligaciones legales, estatutarias, normativas o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.

18.1.1 Identificación de los requisitos de legislación y contractuales correspondientes

Control

Todos los requisitos estatutarios, normativos y contractuales legislativos y el enfoque de la organización para cumplir con estos requisitos de deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y la organización.

Orientación sobre la implementación

Los controles específicos y las responsabilidades individuales para cumplir con estos requisitos también se deberían definir y documentar.

Los gerentes deberían identificar toda la legislación que se aplica a su organización para poder cumplir con los requisitos para su tipo de negocio. Si la organización realiza negocios en otros países, los gerentes deberían considerar el cumplimiento en todos los países pertinentes.

18.1.2 Derechos de propiedad intelectual

Control

Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos de software propietario.

Orientación sobre la implementación

Se deberían considerar las siguientes pautas para proteger a cualquier material que se puede considerar como propiedad intelectual:

a) la publicación de una política de cumplimiento de derechos de propiedad intelectual que define el uso legal de software y productos de información;

b) la adquisición de software solo a través de fuentes conocidas y con buena reputación, para garantizar que no se transgreda el derecho de autor;

c) mantener la concientización de las políticas para proteger los derechos de propiedad intelectual dando aviso de la intención de tomar medidas disciplinarias contra el personal que las incumple.

d) mantener registros de activos adecuados y la identificación de todos los activos con los requisitos para proteger los derechos de propiedad intelectual;

e) mantener pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.;

f) implementar controles para garantizar que cualquier número máximo de usuarios permitidos dentro la licencia no se exceda;

g) realización de revisiones para verificar que solo se instale software y productos licenciados;

h) proporcionar una política para mantener las condiciones adecuadas de las licencias;

i) proporcionar una política para eliminar o transferir el software a otros;

j) cumplir con los términos y condiciones para el software y la información obtenida de redes públicas;

k) no duplicar, convertir a otro formato ni extraer de grabaciones comerciales (película, audio) a no ser que lo permita la ley de derecho de autor;

l) no copiar libros, artículos, informes u otros documentos en su totalidad o en parte, que no sean los permitidos por la ley de derecho de autor.

Otra información

Los derechos de propiedad intelectual incluyen los derechos de autor del software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código de fuente.

Los productos de software propietario generalmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitando el uso de productos a máquinas específicas o limitando la copia a la creación de copias de respaldo solamente. La importancia y el conocimiento de los derechos de propiedad intelectual se deberían comunicar al personal para el desarrollo de software de la organización.

Los requisitos legislativos, normativos y contractuales pueden imponer restricciones en la copia de material propietario. En particular, pueden requerir que se utilice solamente material que desarrolla la organización o que tiene licencia, o que proporciona el desarrollador a la organización. Las infracciones al derecho de autor pueden llevar a acciones legales, que pueden involucrar multas y procesos penales.

18.1.3 Protección de registros

Control

Los registros se deberían proteger contra pérdidas, destrucción, falsificación, acceso no autorizado y publicación no autorizada de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

Orientación sobre la implementación

Al decidir sobre la protección de los registros organizacionales específicos, se debería considerar su clasificación correspondiente en base al esquema de clasificación de la organización. Los registros se deberían categorizar en tipos de registros, es decir, 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 medios de almacenamiento permitidos, es decir, papel, microficha, magnético, óptico. Cualquier clave y programa criptográfico relacionado asociado a los archivos cifrados o firmas digitales (ver cláusula 10), se debería almacenar para permitir la descripción de los registros por el tiempo en que se retengan los registros.

Se debería tener en consideración la posibilidad del deterioro de los medios que se utilizan para el almacenamiento de registros. Se deberían implementar procedimientos de almacenamiento y manipulación de acuerdo con las recomendaciones del fabricante.

Donde se elijan medios de almacenamiento electrónico, se deberían establecer procedimientos para garantizar la capacidad de acceder a los datos (legibilidad de medios y formato) por todo el período de retención para protegerlos contra la pérdida debido a cambios en la futura tecnología.

Se deberían seleccionar sistemas de almacenamiento de datos para que se puedan recuperar los datos en un período de tiempo y formato aceptable, en función de los requisitos que se deberían cumplir.

El sistema de almacenamiento y manipulación debería garantizar la identificación de registros y su período de retención según lo define la legislación y las normativas nacionales y regionales, si corresponde. Este sistema debería permitir la destrucción adecuada de los registros después de ese período si la organización ya no los necesita.

Para cumplir con estos objetivos de resguardo de registros, se deberían realizar los siguientes pasos dentro de una organización:

a) se deberían emitir pautas sobre la retención, el almacenamiento, el manejo y la eliminación de los registros y de la información;

b) se debería establecer un programa de retención que identifique los registros y el período de tiempo en el que se deberían retener;

c) se debería mantener un inventario de las fuentes de información clave.

Otra información

Es posible que se deban retener algunos registros de manera segura para cumplir con los requisitos estatutarios o contractuales, así como también para apoyar actividades comerciales esenciales. Algunos ejemplos incluyen registros que pueden ser necesarios como evidencia de que una organización opera dentro de las reglas estatutarias o normativas, para garantizar la defensa contra posibles acciones penales o civiles o para confirmar el estado financiero de una organización a los accionistas, partes externas y auditores. La ley o normativa nacional puede establecer el período de tiempo y el contenido de datos para la retención de la información.

Puede encontrar más información sobre la administración de los registros organizacionales en ISO 15489-1.

18.1.4 Privacidad y protección de información personal identificable

Control

Se debería garantizar la privacidad y la protección de la información personal identificable según se requiere en la legislación y las normativas pertinentes donde corresponda.

Orientación sobre la implementación

Se debería desarrollar e implementar una política de datos de la organización para la privacidad y protección de la información personal identificable. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información personal identificable.

El cumplimiento con esta política y toda la legislación y normativas pertinentes sobre la protección de la privacidad de las personas y la protección de la información personal identificable requiere la estructura y control de administración adecuada. A menudo esto se logra de mejor manera mediante la asignación de una persona responsable, como un funcionario encargado de la privacidad, quien debería brindar orientación a los gerentes, usuarios y proveedores de servicio sobre sus responsabilidades individuales y procedimientos

específicos que se deberían seguir. La responsabilidad de manejar información personal identificable y de garantizar el conocimiento de los principios de privacidad se debería abordar de acuerdo con la legislación y las normativas pertinentes. Se deberían implementar las medidas técnicas y organizacionales adecuadas para proteger la información personal identificable.

Otra información

ISO/IEC 29100 proporciona un marco de alto nivel para la protección de información personal identificable dentro de los sistemas de tecnología de información y comunicación. Ciertos países han introducido controles de legislación sobre la recopilación, el procesamiento y la transmisión de información personal identificable (generalmente la información que yace en personas que se pueden identificar a partir de esa información). En función de la legislación nacional correspondiente, dichos controles pueden imponer deberes en aquellas personas que recopilan, procesan y diseminan información personal identificable y también pueden restringir la capacidad de transferir información personal identificable a otros países.

18.1.5 Regulación de controles criptográficos

Control

Se deberían utilizar controles criptográficos en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

Orientación sobre la implementación

Se deberían considerar los siguientes elementos para el cumplimiento con los acuerdos, las leyes y normativas pertinentes:

a) restricciones sobre la importación o exportación de hardware y software informático para realizar funciones criptográficas;

b) las restricciones sobre la importación o la exportación sobre el hardware y software informático que está diseñado para tener funciones criptográficas agregadas;

c) restricciones sobre el uso del cifrado;

d) métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información cifrada por hardware o software para proporcionar la confidencialidad del contenido.

Se debería buscar asesoría legal para garantizar el cumplimiento con la legislación y las normativas pertinentes. Antes de que se mueva la información cifrada o los controles criptográficos a través de las fronteras jurisdiccionales, también se debería buscar asesoría legal.

18.2 Revisiones de la seguridad de la información

Objetivo: garantizar que se implementa y opera la seguridad de la información de acuerdo a las políticas y procedimientos organizacionales.

18.2.1 Revisión independiente de la seguridad en la información

Control

El enfoque de la organización para administrar la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) se deberían revisar independientemente en intervalos planificados o cuando ocurren cambios significativos.

Orientación sobre la implementación

La dirección debería iniciar la revisión independiente. Una revisión independiente es necesaria para asegurar la idoneidad, adecuación y efectividad continua del enfoque de la organización para administrar la seguridad de la información. La revisión debería incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluidos los objetivos de política y control.

Dicha revisión la deberían realizar personas independientes del área bajo revisión, es decir, la función de auditoría interna, un gerente independiente o una organización externa que se especialice en dichas revisiones. Las personas que realizan estas revisiones deberían contar con las habilidades y experiencia adecuada.

Los resultados de la revisión independiente se deberían registrar e informar a la dirección que inició esta revisión. Se deberían mantener estos registros.

Si la revisión independiente identifica que el enfoque y la implementación de la organización para administrar la seguridad de la información es inadecuada, es decir, que no se cumplen los objetivos y requisitos adecuados o que no cumplen con la indicación de seguridad de la información establecida en las políticas de seguridad de la información (ver 5.1.1), la dirección debería considerar tomar medidas correctivas.

Otra información

ISO/IEC 27007, *Guidelines for information security management systems auditing* e ISO/IEC TR 27008, *Guidelines for auditors on information security controls* también brindan orientación para realizar la revisión independiente.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Control

Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad con las políticas, normas y cualquier otro tipo de requisitos de seguridad correspondientes.

Orientación sobre la implementación

Los gerentes deberían identificar cómo verificar que se cumplen esos requisitos de seguridad de la información definidos en las políticas, normas y otras normativas pertinentes. Se debería considerar la medición automática y herramientas de informes para la revisión regular eficiente.

Si se encuentra cualquier falta de cumplimiento como resultado de la revisión, los gerentes deberían:

a) identificar las causas del incumplimiento;

b) evaluar la necesidad que tienen las acciones para lograr el cumplimiento;

c) implementar acciones correctivas adecuadas;

d) revisar la acción correctiva tomada para verificar su efectividad e identificar cualquier tipo de deficiencias y falencias.

Los resultados de las revisiones y acciones correctivas que realizan los gerentes se deberían registrar y se deberían mantener estos registros. Los gerentes deberían informar los resultados a las personas que realizan revisiones independientes (ver 18.2.1) cuando se realiza una revisión independiente en el área de su responsabilidad.

Otra información

El uso del monitoreo operacional del sistema se cubre en 12.4.

18.2.3 Revisión de cumplimiento técnico

Control

Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad de la información de la organización.

Orientación sobre la implementación

El cumplimiento técnico se debería revisar de preferencia con la asistencia de herramientas automatizadas, que generan informes técnicos para la interpretación posterior por parte de un especialista técnico. De manera alternativa, un ingeniero en sistemas con experiencia puede realizar revisiones manuales (con el apoyo de herramientas de software correspondientes, en caso de ser necesario).

Si se utilizan pruebas de penetración o evaluaciones de vulnerabilidad, se debería tener precaución, pues tales actividades podrían comprometer la seguridad del sistema. Esas pruebas se deberían planificar, documentar y deberían ser repetibles.

Cualquier tipo de revisión de cumplimiento técnico solo deberían realizarlas personas autorizadas competentes o personas que estén bajo la supervisión de dichas personas.

Otra información

Las revisiones de cumplimiento técnico involucran el análisis de los sistemas operacionales para asegurarse de que se han implementado correctamente los controles de hardware y software. Este tipo de revisión de cumplimiento requiere la experiencia técnica de un especialista.

Las revisiones de cumplimiento también abarcan, por ejemplo, las pruebas de penetración y las evaluaciones de vulnerabilidad, que pueden realizarlas expertos independientes que se han contratado específicamente para este fin. Esto puede ser útil para detectar las vulnerabilidades en el sistema y para inspeccionar cuan eficaces son los controles para evitar el acceso no autorizado debido a estas vulnerabilidades.

Las evaluaciones de pruebas de penetración y vulnerabilidades brindan una visión global de un sistema en un estado específico y en un período de tiempo específico. La visión global se limita a aquellas porciones del sistema que se prueban durante los intentos de penetración. Las pruebas de penetración y las evaluaciones de vulnerabilidad no son un sustituto para la evaluación de riesgos.

ISO/IEC TR 27008 brinda una orientación específica en cuanto a las revisiones de cumplimiento técnico.

Anexo A
(informativo)

Bibliografía

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1 *Information technology Security techniques - Key management - Part 1: Framework.*

[3] ISO/IEC 11770-2 *Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques.*

[4] ISO/IEC 11770-3 *Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques.*

[5] ISO 15489-1 *Information and documentation - Records management - Part 1: General.*

[6] ISO/IEC 20000-1 *Information technology - Service management - Part 1: Service management system requirements.*

[7] ISO/IEC 20000-2 *Information technology - Service management - Part 2: Guidance on the application of service management systems.*

[8] ISO 22301 *Societal security - Business continuity management systems - Requirements.*

[9] ISO 22313 *Societal security - Business continuity management systems - Guidance.*

[10] ISO/IEC 27001 *Information technology - Security techniques - Information security management systems - Requirements.*

[11] ISO/IEC 27005 *Information technology - Security techniques - Information security risk management.*

[12] ISO/IEC 27007 *Information technology - Security techniques - Guidelines for information security management systems auditing.*

[13] ISO/IEC TR 27008 *Information technology - Security techniques - Guidelines for auditors on information security controls.*

[14] ISO/IEC 27031 *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.*

[15] ISO/IEC 27033-1 *Information technology - Security techniques - Network security - Part 1: Overview and concepts.*

[16] ISO/IEC 27033-2 *Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security.*

[17] ISO/IEC 27033-3 *Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues.*

[18] ISO/IEC 27033-4 *Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways.*

[19] ISO/IEC 27033-5 *Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Network (VPNs).*

[20] ISO/IEC 27035 *Information technology - Security techniques - Information security incident management.*

[21] ISO/IEC 27036-1 *Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts.*

[22] ISO/IEC 27036-2 *Information technology - Security techniques - Information security for supplier relationships - Part 2: Common requirements.*

[23] ISO/IEC 27036-3 *Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security.*

[24] ISO/IEC 27037 *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence.*

[25] ISO/IEC 29100 *Information technology - Security techniques - Privacy framework.*

[26] ISO/IEC 29101 *Information technology - Security techniques - Privacy architecture framework.*

[27] ISO 31000 *Risk management - Principles and guidelines.*

NOTA EXPLICATIVA NACIONAL

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 11770-1	No hay	-
ISO/IEC 11770-2	No hay	-
ISO/IEC 11770-3	No hay	-
ISO 15489-1	NCh-ISO 15489/1:2010	La Norma Chilena NCh-ISO 15489:2010 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO 15489-1:2001.
ISO/IEC 20000-1	NCh-ISO 20000/1:2013	La Norma Chilena NCh-ISO 20000/1:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 20000-1:2011.
ISO/IEC 20000-2	NCh-ISO 20000/2:2013	La Norma Chilena NCh-ISO 20000/2:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 20000-2:2012.

(continúa)

(conclusión)

ISO 22301	NCh-ISO 22301:2013	La Norma Chilena NCh-ISO 22301:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO 22301:2012.
ISO 22313	En estudio	
ISO/IEC 27001	NCh-ISO 27001:2013	La Norma Chilena NCh-ISO 27001:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27001:2013.
ISO/IEC 27005	NCh-ISO 27005:2009	La Norma Chilena NCh-ISO 27005:2009 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27005:2008.
ISO/IEC 27007	NCh-ISO 27007:2012	La Norma Chilena NCh-ISO 27007:2012 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC FDIS 27007:2011.
ISO/IEC TR 27008	No hay	-
ISO/IEC 27031	No hay	-
ISO/IEC 27033-1	No hay	-
ISO/IEC 27033-2	No hay	-
ISO/IEC 27033-3	No hay	-
ISO/IEC 27033-4	No hay	-
ISO/IEC 27033-5	No hay	-
ISO/IEC 27035	No hay	-
ISO/IEC 27036-1	No hay	-
ISO/IEC 27036-2	No hay	-
ISO/IEC 27036-3	No hay	-
ISO/IEC 27037	No hay	-
ISO/IEC 29100	No hay	-
ISO/IEC 29101	No hay	-
ISO 31000	NCh-ISO 31000:2012	La Norma Chilena NCh-ISO 31000:2012 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO 31000:2009.

Anexo B
(informativo)

Justificación de los cambios editoriales

Tabla B.1 - Cambios editoriales

Cláusula/subcláusula	Cambios editoriales	Justificación
En toda la norma	Se reemplaza "esta Norma Internacional" por "esta norma".	La norma es de alcance nacional.
1	Se reemplaza "Alcance" por "Alcance y campo de aplicación".	De acuerdo a estructura de NCh2.
2 y Anexo A	Se agrega Nota Explicativa Nacional.	Para detallar la equivalencia y el grado de correspondencia de las Normas Internacionales con las Normas Chilenas.

ICS 35.040