# INSTITUTO ECUATORIANO DE NORMALIZACIÓN

Quito - Ecuador

## NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27002:2009

**NÚMERO DE REFERENCIA ISO/IEC 27002:2005 (E)**

# TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE LA SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

**Primera Edición**

INFORMATION TECHNOLOGY-SECURITY TECHNIQUES-CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT.

First Edition

DESCRIPTORES: Tecnología de la información, grupos de caracteres y códigos de información, gestión de la seguridad de la información; evaluación de riesgos; sistemas de gestión

TI 01.01-601
CDU: 65.012.8
CIIU: 0000
ICS: 35.040

**Contenido** **Página**

## Prólogo

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

Los estándares internacionales son delineados de acuerdo con las reglas dadas en las Directivas ISO/IEC, Parte 2

La principal tarea del comité técnico conjunto es preparar Estándares Internacionales. Los Estándares Internacionales delineados adoptados por el comité técnico conjunto son entregados a los organismos nacionales para votación. La publicación como un Estándar Internacional requiere la aprobación de al menos 75% de los organismos nacionales que otorgan el voto.

Se alerta de la posibilidad que algunos de los elementos de este documento puedan ser sujetos de derechos de patentes. ISO y IEC no serán responsables de identificar ninguno o todos los derechos de tales patentes.

ISO/IEC 27002 fue preparado por el Comité Técnico ISO/IEC JTC1, Tecnologías de la Información, Sucomité SC 27, IT (Security Techniques) Tecnología de seguridad.

La primera edición de la ISO/IEC 27002 fue preparado por el Comité Técnico ISO/IEC 17799:2005 y ISO/IEC 17799:2005 /Cor.1:2007. Su contenido técnico es idéntico a la ISO/IEC 17799:2005 y ISO/IEC 17799:2005 /Cor.1:2007. Cambia el número de referencia de la norma 17799 a 27002. La ISO/IEC 17799:2005 y la ISO/IEC 17799:2005/Cor.1:2007 provisionalmente se archiva hasta la segunda edición de la ISO/IEC 27002

## 0. INTRODUCCIÓN

### 0.1 ¿Qué es la seguridad de la información?

La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades una organización y, en consecuencia, necesita una protección adecuada. Esto es especialmente importante en el entorno del negocio cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades (véase también OECD Guía para la seguridad de redes y sistemas de información).

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de inversiones y oportunidades del negocio.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen los objetivos específicos de la seguridad y del negocio una organización. Esto debería hacerse en conjunto con otros procesos de gestión del negocio.

### 0.2 ¿Por qué es necesaria la seguridad de la información?

La información y los procesos, sistemas y redes que la soportan son activos importantes del negocio. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para mantener su competitividad, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial. Las organizaciones y sus sistemas y redes de información enfrentan amenazas de la seguridad procedentes de una gran variedad de fuentes, incluyendo fraudes asistidos por computador, espionaje, sabotaje, vandalismo, incendios o inundaciones. Las causas de daño tales como códigos maliciosos y ataques de piratería por computador y negación del servicio se han vuelto más comunes, más ambiciosos y cada vez más sofisticados.

La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información actuará como un elemento facilitador, por ejemplo para lograr, gobierno en línea (*e-government*) o negocios electrónicos (*e-business*) y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia hacia la computación distribuida también ha debilitado la eficacia del control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que se puede lograr a través de los medios técnicos es limitada y debería estar soportada por una buena gestión y por procedimientos apropiados. La identificación de los controles que se deberían establecer requiere planificación y atención cuidadosa a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de todos los empleados una organización. También puede requerir la participación de accionistas, proveedores, terceras partes, clientes u otras partes externas. De igual modo puede ser necesaria la asesoría especializada de organizaciones externas.

### 0.3 ¿Cómo establecer los requisitos de la seguridad?

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

*(Continúa)*

1) Una fuente se deriva de una evaluación de los riesgos para la organización, teniendo en cuenta la estrategia y los objetivos globales del negocio. A través de una evaluación de riesgos, se identifican las amenazas para los activos, se evalúan la vulnerabilidad y la probabilidad de ocurrencia y se estima el impacto potencial.

2) Otra fuente son los requisitos legales, estatutarios, reglamentarios y contractuales que debe cumplir la organización, sus socios comerciales, los contratistas y los proveedores de servicios, así como su entorno socio-cultural.

3) Una fuente adicional es el conjunto particular de principios, objetivos y requisitos del negocio para el procesamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

**0.4 Evaluación de los riesgos de la seguridad**

Los requisitos de la seguridad se identifican mediante una evaluación metódica de los riesgos de la seguridad. Los gastos en los controles se deben equilibrar frente a la probabilidad de daño para el negocio que resulta de las fallas en la seguridad.

Los resultados de una evaluación de riesgos ayudarán a guiar y a determinar la acción de gestión adecuada y las prioridades para la gestión de los riesgos de la seguridad de la información, así como para implementar los controles seleccionados para la protección contra estos riesgos.

Una evaluación de riesgos se debería repetir periódicamente para tratar cualquier cambio que pueda influir en los resultados de una evaluación de riesgos.

Información adicional sobre una evaluación de los riesgos de la seguridad se puede encontrar en el numeral 4.1, "Evaluación de los riesgos de la seguridad".

**0.5 Selección de controles**

Una vez que se han identificado los requisitos y los riesgos de la seguridad y se han tomado las decisiones para el tratamiento de los riesgos, es conveniente seleccionar e implementar los controles para garantizar la reducción de los riesgos hasta un nivel aceptable. Los controles se pueden seleccionar a partir de este documento, de otros grupos de controles o se pueden diseñar controles nuevos para satisfacer necesidades específicas, según sea adecuado. La selección de los controles de la seguridad depende de las decisiones de una organización basadas en los criterios para la aceptación del riesgo, el tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado en la organización, y debería estar sujeta a toda la legislación y todos los reglamentos nacionales e internacionales pertinentes.

Algunos de los controles en esta norma se pueden considerar como principios guía para la gestión de la seguridad de la información y aplicables a la mayoría de las organizaciones. Éstos se explican con más detalle bajo el encabezado "Punto de partida para la seguridad de la información".

Información adicional sobre la selección de controles y otras opciones de tratamiento de riesgos se puede encontrar en el numeral 4.2 "Tratamiento de los riesgos de la seguridad".

**0.6 Punto de partida para la seguridad de la información**

Algunos controles se pueden considerar un buen punto de partida para la implementación de la seguridad de la información. Ellos se basan en requisitos legales esenciales o se consideran una práctica común para la seguridad de la información.

Los controles considerados esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación que se aplique, los siguientes:

a) protección de datos y privacidad de la información personal (véase el numeral 15.1.4);

*(Continúa)*

b) protección de los registros una organización (véase el numeral 15.1.3);

c) derechos de propiedad intelectual (véase el numeral 15.1.2).

Los controles que se consideran una práctica común para la seguridad de la información incluyen los siguientes:

a) documento de la política de la seguridad de la información (véase el numeral 5.1.1);

b) asignación de responsabilidades para la seguridad de la información (véase el numeral 6.1.3);

c) educación, formación y concienciación sobre la seguridad de la información (véase el numeral 8.2.2);

d) procesamiento correcto en las aplicaciones (véase el numeral 12.2);

e) gestión de la vulnerabilidad técnica (véase el numeral 12.6);

f) gestión de la continuidad del negocio (véase el numeral 14);

g) gestión de los incidentes de la seguridad de la información y las mejoras (véase el numeral 13.2).

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

Es conveniente observar que aunque todos los controles en esta norma son importantes y se deberían tener presentes, la pertinencia de cualquier control se debería determinar a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque anterior se considera un buen punto de partida, no reemplaza la selección de controles con base en una evaluación de riesgos.

**0.7 Factores críticos para el éxito**

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

a) políticas, objetivos y actividades de la seguridad de la información que reflejen los objetivos del negocio;

b) un enfoque y un marco de trabajo para implementar, mantener, monitorear y mejorar la seguridad de la información, que sean consistentes con la cultura de una organización;

c) soporte y compromiso visibles en todos los niveles de una organización;

d) una buena comprensión de los requisitos de la seguridad de la información, una evaluación de riesgos y la gestión del riesgo;

e) mercadeo eficaz de la seguridad de la información para todos los directores, empleados y otras partes para lograr la concienciación;

f) distribución de guías sobre la política y las normas de la seguridad de la información a todos los directores, empleados y otras partes;

g) provisión de fondos para actividades de gestión de la seguridad de la información;

h) formación, educación y concienciación adecuadas;

i) establecimiento de un proceso eficaz para la gestión de los incidentes de la seguridad de la información,

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

*(Continúa)*

### 0.8 Desarrollo de directrices propias

Este código de práctica se puede considerar como un punto de partida para el desarrollo de directrices específicas de una organización. No todos los controles ni directrices en este código de práctica se pueden aplicar. Además, se pueden requerir controles y directrices adicionales que no se incluyen en esta norma. Cuando se desarrollan documentos que contienen directrices o controles adicionales puede ser útil incluir referencias cruzadas a numerales de esta norma que faciliten la verificación del cumplimiento por parte de auditores y socios del negocio.

1) Observe que las mediciones de la seguridad de la información están fuera del alcance de esta norma.

*(Continúa)*

CDU: 65.012.8
ICS: 35.040

CIIU: 0000
TI 01.01-601

| Norma Técnica Ecuatoriana Voluntaria | TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE LA SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. | NTE INEN-ISO 27002:2009 2009-05 |
|---|---|---|



## 1. Objeto

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por una evaluación de riesgos.

Esta norma puede servir como guía práctica para el desarrollo de normas de la seguridad de una organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

## 2. Términos y definiciones

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

**2.1**
**activo**
cualquier cosa que tenga valor para la organización.
[ISO/IEC 13335-1:2004]

**2.2**
**control**
medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras una organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
NOTA Control también se usa como sinónimo de salvaguarda o contramedida.

**2.3**
**directriz**
descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
[ISO/IEC 13335-1:2004]

**2.4**
**servicios de procesamiento de información**
cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

**2.5**
**seguridad de la información**
preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

**2.6**
**evento de la seguridad de la información**
un evento de la seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de la seguridad de la información, o falla de controles, o una situación previamente desconocida que puede ser importante para la seguridad.
[ISO/IEC TR 18044:2000]

*(Continúa)*

DESCRIPTORES: Tecnología de la información, grupos de caracteres y códigos de información, gestión de la seguridad de la información; evaluación de riesgos; sistemas de gestión

**2.7**
**incidente de la seguridad de la información**
un incidente de la seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de la seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
[ISO/IEC TR 18044:2000]

**2.8**
**política**
toda intención y directriz expresada formalmente por la Dirección.

**2.9**
**riesgo**
combinación de la probabilidad de un evento y sus consecuencias.
[ISO/IEC Guía 73:2002]

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

**2.11**
**evaluación de riesgos**
Todo proceso de análisis y valoración del riesgo.
[ISO/IEC Guía 73:2002]

**2.12**
**valoración del riesgo**
proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.
[ISO/IEC Guía 73:2002]

**2.13**
**gestión del riesgo**
actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
[ISO/IEC Guía 73:2002]

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

**2.15**
**tercera parte**
persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
[ISO/IEC Guía 2:1996].

**2.16**
**amenaza**
causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
[ISO/IEC 13335-1:2004]

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

*(Continúa)*

## 3. Estructura de esta norma

Esta norma contiene 11 secciones sobre controles de la seguridad que en conjunto tienen un total de 39 categorías principales de la seguridad y una sección de introducción a una evaluación y el tratamiento del riesgo.

### 3.1 Cláusulas

Cada cláusula contiene una cantidad de categorías principales de la seguridad. Estas 11 cláusulas (acompañadas por la cantidad de categorías principales de la seguridad incluida en cada numeral) son:

a) Política de la seguridad (1).

b) Organización de la seguridad de la información (2).

c) Gestión de activos (2).

d) Seguridad de los recursos humanos (3).

e) Seguridad física y del entorno (2).

f) Gestión de operaciones y comunicaciones (10).

g) Control del acceso (7).

h) Adquisición, desarrollo y mantenimiento de sistemas de información (6).

i) Gestión de los incidentes de la seguridad de la información (2).

j) Gestión de la continuidad del negocio (1).

k) Cumplimiento (3).

*Nota El orden de las cláusulas no implica su importancia. Dependiendo de las circunstancias, todas las cláusulas podrían ser importantes, por lo tanto cada organización que aplique esta norma debería identificar las cláusulas aplicables, su importancia y su aplicación a procesos individuales del negocio. Igualmente, ninguna de las listas de esta norma está en orden prioritario, a menos que así se indique.*

### 3.2 Categorías principales de la seguridad

Cada categoría principal de la seguridad contiene:

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

Las descripciones de los controles tienen la siguiente estructura:

*Control*
Define la declaración específica del control para cumplir el objetivo de control.

*Guía de implementación*
Suministra información más detallada para apoyar la implementación del control y satisfacer el objetivo de control. Algunas partes de esta guía pueden no ser adecuadas en todos los casos y por ello pueden ser más apropiadas otras formas de implementación del control.

*Información adicional*
Suministra información que puede ser necesario considerar, por ejemplo las consideraciones legales y las referencias a otras normas.

*(Continúa)*

# 4. Evaluación y tratamiento del riesgo

## 4.1 Evaluación de los riesgos de la seguridad

Una evaluación de riesgos debería identificar, cuantificar y priorizar los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización. Los resultados deberían guiar y determinar la acción de gestión adecuada y las prioridades tanto para la gestión de los riesgos de la seguridad de la información como para implementar los controles seleccionados para la protección contra estos riesgos. Puede ser necesario llevar a cabo el proceso de evaluación de los riesgos y la selección de controles varias veces para cubrir diferentes partes de la organización o sistemas individuales de información.

Es recomendable que una evaluación de riesgos incluya el enfoque sistemático para estimar la magnitud de los riesgos (análisis del riesgo) y el proceso de comparación de los riesgos estimados frente a los criterios de riesgo para determinar la importancia de los riesgos (valoración del riesgo).

Es conveniente realizar periódicamente las evaluaciones de riesgos para abordar los cambios en los requisitos de la seguridad y en la situación de riesgo, por ejemplo en activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando se producen cambios significativos.

Estas evaluaciones de riesgos se deberían efectuar de forma metódica que puedan producir resultados comparables y reproducibles.

Una evaluación de los riesgos de la seguridad de la información debería tener un alcance definido claramente para que sea eficaz y debería incluir las relaciones con las evaluaciones de riesgos en otras áreas, según sea apropiado.

El alcance de una evaluación de riesgos puede abarcar a toda la organización, partes de la organización, un sistema individual de información, componentes específicos del sistema o servicios, cuando es factible, realista y útil. En la norma ISO/IEC TR 13335-3 (Directrices para la seguridad de la tecnología de la información: técnicas para la gestión de la seguridad de la tecnología de la información) se discuten ejemplos de metodologías para una evaluación del riesgo.

## 4.2 Tratamiento de los riesgos de la seguridad

Antes de considerar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar si se pueden aceptar o no los riesgos. Los riesgos se pueden aceptar si, por ejemplo, según una evaluación se considera el riesgo bajo o que el costo del tratamiento no es efectivo en términos financieros para la organización. Tales decisiones se deberían registrar.

Para cada uno de los riesgos identificados después de una evaluación de riesgos es necesario tomar una decisión para su tratamiento. Las opciones posibles para el tratamiento del riesgo incluyen:

a) aplicación de los controles apropiados para reducir los riesgos;

b) aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política de la organización y sus criterios para la aceptación del riesgo;

c) prevención de los riesgos al no permitir acciones que pudieran hacer que éstos se presentaran;

d) transferencia de riesgos asociados a otras partes, por ejemplo aseguradores o proveedores.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se deberían seleccionar e implementar de modo que satisfagan los requisitos identificados por una evaluación de riesgos. Los controles deberían garantizar la reducción de los riesgos hasta un nivel aceptable teniendo en cuenta los siguientes elementos:

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

b) objetivos de la organización;

c) requisitos y restricciones operativos;

*(Continúa)*

d) costo de la implementación y la operación con relación a la reducción de los riesgos, y que se mantenga proporcional a los requisitos y restricciones de la organización;

e) necesidad de equilibrar la inversión en la implementación y operación de los controles frente a la probabilidad del daño que resultara debido a las fallas de la seguridad.

Los controles se pueden seleccionar a partir de esta norma, de otros conjuntos de controles, o se pueden diseñar controles nuevos que satisfagan las necesidades específicas de la organización. Es necesario reconocer que es posible que algunos controles no se puedan aplicar a todos los sistemas y entornos de la información, y pueden no ser viables para todas las organizaciones. A modo de ejemplo, el numeral 10.1.3 describe la forma en que se pueden separar las funciones para evitar fraude y error. Es posible que las organizaciones pequeñas no puedan separar todas las funciones y que sean necesarias otras formas de lograr el mismo objetivo de control. En otro ejemplo, el numeral 10.10 describe la forma en que se puede monitorear el uso del sistema y recolectar evidencia. Los controles descritos, como el registro de eventos, pueden entrar en conflicto con la legislación correspondiente, como por ejemplo en la protección de la privacidad para los clientes o en el sitio de trabajo.

Los controles de la seguridad de la información se deberían tener en cuenta en la especificación de los requisitos de sistemas y proyectos y en la fase de diseño. De lo contrario, se pueden originar costos adicionales y soluciones menos eficaces y, es posible, en el peor de los casos, la incapacidad de lograr una seguridad adecuada.

Se debe recordar que ningún conjunto de controles puede lograr la seguridad completa y que se deberían implementar acciones adicionales de gestión para monitorear, valorar y mejorar la eficiencia y la eficacia de los controles de la seguridad para apoyar las metas de la organización.

# 5. Política de la seguridad

## 5.1 Política de la seguridad de la información

Objetivo: brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de la seguridad de la información en toda la organización.

### *5.1.1 Documento de la política de la seguridad de la información*

*Control*
La dirección debería aprobar un documento de política de la seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

*Guía de implementación*
El documento de la política de la seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de ésta para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

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

b) una declaración de la intención de la dirección, que apoye las metas y los principios de la seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio;

*(Continúa)*

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

d) una explicación breve sobre las políticas, los principios, las normas de la seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización incluyendo los siguientes:

1) cumplimiento de los requisitos legales, reglamentarios y contractuales;

2) requisitos de educación, formación y concienciación sobre seguridad;

3) gestión de la continuidad del negocio;

4) consecuencias de las violaciones de la política de la seguridad;

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

f) referencias a la documentación que puede dar soporte a la política, por ejemplo políticas de la seguridad más detalladas y procedimientos para sistemas específicos de información o las reglas de la seguridad que deberían cumplir los usuarios.

Esta política de la seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

*Información adicional*
La política de la seguridad de la información podría formar parte de un documento de política general. Si la política de la seguridad de la información se distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible. Información adicional se puede encontrar en la ISO/IEC 13335-1:2004.

***5.1.2 Revisión de la política de la seguridad de la información***

*Control*
La política de la seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

*Guía de implementación*
La política de la seguridad de la información debería tener un responsable aprobado por la dirección para el desarrollo, la revisión y la valoración de dicha política.

Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de la seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de la seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

a) retroalimentación de las partes interesadas;

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

c) estados de las acciones preventivas y correctivas (véanse los numerales 6.1.8 y 15.2.1);

d) resultados de las revisiones previas por parte de la dirección;

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

*(Continúa)*

f) cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico;

g) tendencias relacionadas con las amenazas y las vulnerabilidades;

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

i) recomendaciones de las autoridades pertinentes (véase el numeral 6.1.6).

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

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

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

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

Es recomendable mantener un registro de la revisión por la dirección.

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

# 6. Organización de la seguridad de la información

## 6.1 Organización interna

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

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

La dirección debería aprobar la política de la seguridad de la información, asignar las funciones de la seguridad, coordinar y revisar la implementación de la seguridad en toda la organización.

Si es necesario, se recomienda establecer una fuente de asesoría especializada sobre seguridad de la información y ponerla a disposición en la organización. Es conveniente desarrollar contactos con grupos o especialistas externos en seguridad, incluyendo las autoridades pertinentes, para ir al compás de las tendencias industriales, monitorear normas y métodos de evaluación, así como proveer puntos adecuados de vínculo cuando se manejan incidentes de la seguridad de la información. Se debería promover un enfoque multidisciplinario para la seguridad de la información.

### *6.1.1 Compromiso de la dirección con la seguridad de la información*

*Control*
La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información.

*Guía de implementación*
La dirección debería:

a) asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes;

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

*(Continúa)*

c) revisar la eficacia de la implementación de la política de la seguridad de la información;

d) proporcionar un rumbo claro y apoyo visible para las iniciativas de la seguridad;

e) proporcionar los recursos necesarios para la seguridad de la información;

f) aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización;

g) iniciar planes y programas para mantener la concienciación sobre la seguridad de la información;

h) asegurar la coordinación en toda la organización de la implementación de los controles de la seguridad de la información.

La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.

Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor o a través de un organismo de dirección ya existente, como por ejemplo el consejo de directores.

*Información adicional*
Otra información adicional se puede encontrar en ISO/IEC 13335-1:2004.

***6.1.2 Coordinación de la seguridad de la información***

*Control*
Las actividades de la seguridad de la información deberían ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.

*Guía de implementación*
Comúnmente, la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de la seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgos.

Esta actividad debería:

a) garantizar que las actividades de la seguridad se efectúan en cumplimiento de la política de la seguridad de la información;

b) identificar la forma de manejar los no cumplimientos;

c) aprobar metodologías y procesos para la seguridad de la información, como una evaluación de riesgos y la clasificación de información;

d) identificar cambios significativos de las amenazas y la exposición de la información y de los servicios de procesamiento de la información de las amenazas;

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

f) promover eficazmente la educación, la formación y la concienciación de la seguridad de la información en toda la organización;

g) valorar la información recibida del monitoreo y la revisión de los incidentes de la seguridad de la información, y recomendar las acciones apropiadas para responder a los incidentes identificados de la seguridad de la información.

Si la organización no emplea un grupo específico multifuncional, por ejemplo debido a que dicho grupo no es apropiado para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otro organismo de la dirección o un solo director.

*(Continúa)*

### *6.1.3 Asignación de responsabilidades para la seguridad de la información*

*Control*
Se deberían definir claramente todas las responsabilidades en cuanto a seguridad de la información.

*Guía de implementación*
La asignación de responsabilidades para la seguridad de la información se debería realizar de acuerdo con la política de la seguridad de la información (véase el numeral 5). Se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de la seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se deberían definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de la seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidades de la seguridad asignadas pueden delegar las labores de la seguridad a otros. No obstante, siguen siendo responsables y deberían determinar la ejecución correcta de las labores delegadas.

Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) los activos y los procesos de la seguridad asociados con cada sistema particular se deberían identificar y definir claramente;

b) se debería asignar la entidad responsable de cada activo o proceso de la seguridad, así como documentar esta responsabilidad (véase también el numeral 7.1.2);

c) se deberían definir y documentar claramente los niveles de autorización.

*Información adicional*
En muchas organizaciones se designará un director de la seguridad de la información con toda la responsabilidad por el desarrollo e implementación de la seguridad y para apoyar la identificación de controles.

Sin embargo, la responsabilidad por los recursos y la implementación de controles permanecerá en los directores individuales. Una práctica común es designar un responsable para cada activo, quien se hace responsable de su protección diaria.

### *6.1.4 Proceso de autorización para los servicios de procesamiento de la información*

*Control*
Se debería definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de la información.

*Guía de implementación*
Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de la seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de la seguridad correspondientes;

b) cuando es necesario, el hardware y el software se deberían verificar para asegurar que son compatibles con otros componentes del sistema;

c) la utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles (*laptops*), computadores domésticos o dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y se deberían identificar e implementar los controles necesarios.

*(Continúa)*

***6.1.5 Acuerdos sobre confidencialidad***

*Control*
Se deberían identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

*Guía de implementación*
Los acuerdos de confidencialidad o de no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se puedan hacer cumplir legalmente.

Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) definición de la información que se ha de proteger (por ejemplo la información confidencial);

b) duración esperada del acuerdo, incluyendo los casos en que puede ser necesario mantener la confidencialidad indefinidamente;

c) acciones requeridas cuando se termina un acuerdo;

d) responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer");

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

f) el uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información;

g) derecho de auditar y monitorear las actividades que involucran a la información confidencial;

h) Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial;

i) términos para la devolución o la destrucción de la información al terminar el acuerdo;

j) acciones esperadas a tomar en caso de incumplimiento de este acuerdo.

Con base en los requisitos de la seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de confidencialidad o no-divulgación.

Los acuerdos de confidencialidad o no-divulgación deberían cumplir todas las leyes y las regulaciones que se aplican en la jurisdicción correspondiente (véase el numeral 15.1.1).

Los requisitos para los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

*Información adicional*
Los acuerdos de confidencialidad y de no-divulgación protegen la información de la organización e informan a los que suscriben el acuerdo de confidencialidad, sus responsabilidades para proteger, utilizar y divulgar información de forma responsable y autorizada.

Puede ser necesario que de la organización utilice diferentes formas de acuerdos de confidencialidad y de no-divulgación en circunstancias diferentes.

***6.1.6 Contacto con las autoridades***

*Control*
Se deberían mantener contactos apropiados con las autoridades pertinentes.

*(Continúa)*

*Guía de implementación*
Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

*Información adicional*
El mantenimiento de dichos contactos puede ser un requisito para dar soporte a la gestión de incidentes de la seguridad de la información (véase el numeral 13.2) o a la continuidad del negocio y el proceso de planes de contingencia (véase la sección 14). Los contactos con los organismos de regulación también son útiles para anticipar y preparar los cambios futuros en la ley o en los reglamentos que la organización debe cumplir. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad, como el departamento de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (junto con enrutamiento de línea y disponibilidad) y proveedores de agua (junto con medios de refrigeración para los equipos).

### *6.1.7 Contactos con grupos de interés especiales*

*Control*
Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

*Guía de implementación*
La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

a) mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad;

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

c) recibir advertencias oportunas de alertas, avisos y parches relacionados con ataques y vulnerabilidades;

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

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

f) suministrar puntos adecuados de enlace cuando se trata de incidentes de la seguridad de la información (véase el numeral 13.2.1).

*Información adicional*
Se pueden establecer acuerdos para compartir información con el objeto de mejorar la cooperación y la coordinación de los temas de la seguridad. Dichos acuerdos deberían identificar los requisitos para la protección de la información sensible.

### *6.1.8 Revisión independiente de la seguridad de la información*

*Control*
El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados, o cuando ocurran cambios significativos en la implementación de la seguridad.

*(Continúa)*

*Guía de implementación*
La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir una evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión debería ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o de la organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de la seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información (véase el numeral 5.1.1), la dirección debería considerar las acciones correctivas.

*Información adicional*
El área que los directores deberían revisar regularmente (véase el numeral 15.2.1) también se podría revisar independientemente. Las técnicas de revisión pueden incluir entrevistas de la dirección, verificación de registros o revisión de los documentos de la política de la seguridad. La norma NTE-INEN/ISO 19011:2002, Directrices para la auditoría de los sistemas de gestión ambiental y/o de calidad también puede suministrar una guía útil para llevar a cabo la revisión independiente, incluyendo el establecimiento y la implementación de un programa de revisión.

El numeral 15.3 especifica los controles pertinentes para la revisión independiente de los sistemas de información operativos y el uso de las herramientas de auditoría de sistemas.

## 6.2 Partes externas

**Objetivo:** mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

La seguridad de la información y de los servicios de procesamiento de información no se deberían reducir introduciendo productos o servicios de partes externas.

Se debería controlar todo acceso a los servicios de procesamiento de información, así como el procesamiento y comunicación de información por partes externas.

Cuando existe una necesidad del negocio de trabajar con partes externas que pueden requerir acceso a la información de la organización y a sus servicios de procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte externa, se debería realizar una evaluación de riesgos para determinar las implicaciones para la seguridad y los requisitos de control. Los controles se deberían acordar y definir en un convenio con la parte externa.

### *6.2.1 Identificación de los riesgos relacionados con las partes externas*

*Control*
Se deberían identificar los riesgos para la información y los servicios de procesamiento de información de la organización en los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.

*(Continúa)*

*Guía de implementación*

Cuando existe la necesidad de permitir el acceso de una parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgos (véase también la sección 4) para identificar los requisitos para los controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se deberían considerar los siguientes aspectos:

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

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

1) acceso físico, por ejemplo a oficinas, recintos de computadores y gabinetes de archivos;

2) acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización;

3) conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto;

4) si el acceso tendrá lugar en las instalaciones o fuera de ellas.

c) el valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio;

d) los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas;

e) el personal de la parte externa involucrado en manejar la información de la organización;

f) la forma en que se puede identificar a la organización o al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo;

g) los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información;

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

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

j) los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta;

k) la forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y, cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión o el acceso y el acuerdo de trabajo. En general, todos los requisitos de la seguridad, que resultan del trabajo con partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa (véanse los numerales 6.2.2 y 6.2.3).

Se debería garantizar que la parte externa es consciente de sus obligaciones y acepta las responsabilidades y deberes involucrados en el acceso, procesamiento, comunicación o gestión de la información y los servicios de procesamiento de información de la organización.

*(Continúa)*

*Información adicional*
Las partes externas podrían poner en riesgo la información con una gestión inadecuada de la seguridad. Se deberían identificar y aplicar los controles para administrar el acceso de la parte externa a los servicios de procesamiento de información. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se podrían utilizar los acuerdos de no divulgación.

Las organizaciones pueden enfrentar riesgos asociados con procesos, gestión y comunicación entre las organizaciones, si se aplica un alto grado de contratación externa cuando existen varias partes externas involucradas.

Los controles 6.2.2 y 6.2.3 comprenden diferentes acuerdos con partes externas, incluyendo por ejemplo:

a) proveedores de servicios, como los proveedores de servicios de Internet, proveedores de red, servicios telefónicos, servicios de mantenimiento y soporte;

b) servicios de la seguridad dirigidos;

c) clientes;

d) contratación externa de servicios y/u operaciones, sistemas de tecnología de la información, servicios de recolección de datos, operaciones de centro de llamadas;

e) asesores del negocio y de la gestión, y auditores;

f) desarrolladores y proveedores, por ejemplo productos de software y sistemas de tecnología de la información;

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

h) personal temporal, ubicación de estudiantes y otras asignaciones casuales a corto plazo;

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

***6.2.2 Consideraciones de la seguridad cuando se trata con los clientes***

*Control*
Todos los requisitos de la seguridad identificados se deberían considerar antes de dar acceso a los clientes a los activos o la información de la organización.

*Guía de implementación*
Los siguientes términos se deberían considerar para cubrir la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización (dependiendo del tipo y la extensión de dicho acceso, no se podrían aplicar todos ellos):

a) protección de activos, incluyendo:

   1) procedimientos para proteger los activos de la organización, incluyendo información y software, y gestión de las vulnerabilidades conocidas;

   2) procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de datos;

   3) integridad;

   4) restricciones a la copia y la divulgación de la información;

b) descripción del producto o servicio que se va proveer;

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

*(Continúa)*

d) política de control del acceso, incluyendo:

1) métodos de acceso permitido y control y uso de identificadores únicos tales como la identificación del usuario (ID) y las contraseñas;

2) un proceso de autorización para los privilegios y el acceso de los usuarios;

3) una declaración de que el acceso que no se autorice explícitamente está prohibido;

4) un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;

e) convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de referencias personales), incidentes de la seguridad de la información y violaciones de la seguridad.

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

g) la meta del nivel de servicio y los niveles inaceptables de servicio;

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

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

j) las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con clientes en otros países (véase el numeral 15.1).

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

*Información adicional*
Los requisitos de la seguridad relacionados con los clientes que tiene acceso a los activos de la organización pueden variar considerablemente dependiendo de la información y de los servicios de procesamiento de información a los cuales se tiene acceso. Estos requisitos de la seguridad se pueden abordar empleando acuerdos con el cliente que contengan todos los riesgos y requisitos de la seguridad identificados (véase el numeral 6.2.1).

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a la parte externa deberían incluir la permisividad para la designación de otras partes y las condiciones elegibles para su acceso y participación.

### *6.2.3 Consideraciones de la seguridad en los acuerdos con terceras partes*

*Control*
Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación o gestión de la información o de los servicios de procesamiento de información de la organización, o la adición de productos o servicios a los servicios de procesamiento de la información deberían considerar todos los requisitos pertinentes de la seguridad.

*Guía de implementación*
El acuerdo debería garantizar que no existen malos entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumplir los requisitos de la seguridad identificados:

a) la política de la seguridad de la información;

b) los controles para asegurar la protección del activo, incluyendo:

*(Continúa)*

1) procedimientos para proteger los activos de la organización, incluyendo información, software y hardware;

2) todos los controles y mecanismos de protección física requeridos;

3) controles para asegurar la protección contra software malicioso (véase el numeral 10.4.1);

4) procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware;

5) controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo;

6) confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente de los activos (véase el numeral 6.1.5);

7) restricciones a la copia y a la divulgación de información, y uso de acuerdos de confidencialidad (véase el numeral 6.1.5);

c) la formación del usuario y del administrador en métodos, procedimientos y seguridad;

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

e) las disposiciones para la transferencia de personal, cuando es apropiado;

f) las responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware;

g) la estructura clara y los formatos acordados para la presentación de los informes;

h) el proceso claro y específico para la gestión de cambios;

i) la política de control del acceso, incluyendo:

1) diversas razones, requisitos y beneficios de la necesidad del acceso por terceras partes;

2) métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas;

3) proceso de autorización para los privilegios y el acceso del usuario;

4) requisito para mantener una lista de las personas autorizadas a usar los servicios que se ponen a disposición, y de sus derechos y privilegios con relación a tal uso;

5) declaración de que el acceso que no se autorice explícitamente está prohibido;

6) proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;

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

k) una descripción del producto o servicio que va a ser proporcionado y una descripción de la información que va a estar disponible junto con su clasificación de la seguridad (véase el numeral 7.2.1);

l) la meta del nivel de servicio y los niveles inaceptables de servicio;

m) la definición de criterios verificables de desempeño, su monitoreo y reporte;

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

*(Continúa)*

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

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

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

r) las responsabilidades civiles correspondientes de las partes del acuerdo;

s) las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales, por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con organizaciones en otros países (véase el numeral 15.1);

t) los derechos de propiedad intelectual (DPI) y asignación de derechos de copia (véase el numeral 15.1.2) y la protección de cualquier trabajo colaborativo (véase el numeral 6.1.5);

u) la participación de la tercera parte con los subcontratistas y los controles de la seguridad que estos subcontratistas necesitan implementar;

v) las condiciones para la renegociación / terminación del acuerdo:

1) se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes de la finalización de los acuerdos;

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

3) documentación vigente de las listas de activos, licencias, acuerdos o derechos relacionados con ellos.

*Información adicional*

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de terceras partes. Por lo tanto, se debe tener cuidado al incluir todos los riesgos y requisitos de la seguridad identificados (véase el numeral 6.2.1) en los acuerdos.

Cuando es necesario, los procedimientos y controles requeridos se pueden ampliar en el plan de gestión de la seguridad.

Si la gestión de la seguridad se contrata externamente, los acuerdos deberían abarcar la forma en que la tercera parte garantizará la seguridad adecuada, tal como se definió mediante la evaluación de riesgos, cómo mantendrá la seguridad, y cómo se adaptará la seguridad para identificar y tratar los cambios en los riesgos.

Algunas de las diferencias entre la contratación externa y otras formas de prestación de servicios de terceras partes incluyen el tema de la responsabilidad civil, la planificación del periodo de transición y la interrupción potencial de las operaciones durante este periodo, acuerdos sobre planificación de contingencias y revisiones con la debida diligencia, así como la recolección y gestión de información sobre incidentes de la seguridad. Por ello, es importante que la organización planifique y gestione la transición hacia un acuerdo contratado externamente y tenga procesos adecuados establecidos para la gestión de los cambios y la renegociación / terminación de los acuerdos.

Es necesario considerar en el acuerdo los procedimientos para el procesamiento continuo, en el caso de que la tercera parte no pueda suministrar sus servicios, para evitar cualquier retraso en la provisión de los servicios de reemplazo.

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a la tercera parte deberían incluir la permisividad para la designación de otras partes y las condiciones elegibles para su acceso y participación.

*(Continúa)*

En general, los acuerdos los desarrolla en primer término la organización. Puede haber ocasiones, en algunas circunstancias, en que una tercera parte pueda desarrollar un acuerdo e imponerlo a la organización. Es necesario que la organización garantice que su propia seguridad no sufra impactos innecesarios debido a los requisitos de la tercera parte estipulados en los acuerdos impuestos.

# 7. Gestión de activos

## 7.1 Responsabilidad por los activos

**Objetivo:** lograr y mantener la protección adecuada de los activos de la organización.

Todos los activos se deben incluir y deben tener un responsable designado.

Se deberían identificar los responsables para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los controles específicos puede ser delegada por el responsable, según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.

### *7.1.1 Inventario de activos*

*Control*
Todos los activos deberían estar claramente identificados y se debería elaborar y mantener un inventario de todos los activos importantes.

*Guía de implementación*
La organización debería identificar todos los activos y documentar su importancia. El inventario de activos debería incluir toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio. Este inventario no debería duplicar innecesariamente otros inventarios, pero se debería garantizar que el contenido esté acorde.

Además, se deberían acordar y documentar la propiedad (véase el numeral 7.1.2) y la clasificación de la información (véase el numeral 7.2) para cada uno de los activos. Con base en la importancia del activo, su valor para el negocio y su clasificación de la seguridad se recomienda identificar los niveles de protección según la importancia de los activos (información adicional sobre la forma de valorar los activos para representar su importancia se puede encontrar en la norma ISO/IEC TR 13335-3).

*Información adicional*
Existen muchos tipos de activos, incluyendo:

a) información: bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada;

b) activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;

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

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

e) personas y sus calificaciones, habilidades y experiencia;

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

*(Continúa)*

Los inventarios de activos ayudan a garantizar que se logra la protección eficaz de los activos y también se puede requerir para otros propósitos del negocio como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos). El proceso para obtener un inventario de activos es un prerrequisito importante de la gestión de riesgos (véase el numeral 4).

***7.1.2 Responsable de los activos***

*Control*
Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser asignada a una parte de la organización que actúa como responsable [2]

*Guía de implementación*
El responsable del activo debería responsabilizarse de:

a) garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente;

b) definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

La responsabilidad puede ser designada para:

a) un proceso del negocio;

b) un conjunto definido de actividades;

c) una aplicación;

d) un conjunto definido de datos.

*Información adicional*
Las labores rutinarias se pueden delegar, por ejemplo a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del responsable.

En los sistemas complejos de información puede ser útil asignar grupos de activos que actúan juntos para suministrar una función particular como "servicios". En este caso, el responsable del servicio es responsable de la entrega de éste, incluyendo el funcionamiento de los activos que lo proporcionan.

2) El término "responsable" identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "responsable" no implica que la persona tenga realmente los derechos de propiedad de los activos.

***7.1.3 Uso aceptable de los activos***

*Control*
Se deberían identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

*Guía de implementación*
Todos los empleados, contratistas y usuarios por tercera parte deberían seguir las reglas para el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de información, incluyendo:

a) reglas para el uso del correo electrónico y de Internet (véase el numeral 10.8).

b) directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización (véase el numeral 11.7.1).

[2] El término 'propietario' identifica a un individuo o la entidad que ha aprobado la responsabilidad de controlar la dirección de la producción, el desarrollo, el mantenimiento, el empleo y la seguridad del valor del activo. El término 'propietario' no significa que la persona en realidad tenga cualquier derecho de característica(propiedad) al activo

*(Continúa)*

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de tercera parte que utilizan o tienen acceso a los activos de la organización deberían estar consientes de los límites que existen para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Ellos deberían ser responsables del uso que hagan de los recursos de procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

## 7.2 Clasificación de la información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.
La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

### *7.2.1 Directrices de clasificación*

*Control*
La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

*Guía de implementación*
Las clasificaciones y los controles de protección asociados para la información deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

Las directrices de clasificación deberían incluir convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control del acceso (véase el numeral 11.1.1).

Debería ser responsabilidad del responsable del activo (véase el numeral 7.1.2) definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado. La clasificación debería considerar el efecto de suma mencionado en el numeral 10.7.2.

Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

*Información adicional*
El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad como también otros requisitos para la información en consideración.

Con frecuencia, la información deja de ser sensible o importante después de un periodo de tiempo dado, por ejemplo, cuando la información se hace pública. Se deberían considerar estos aspectos puesto que la superclasificación puede originar la implementación de controles innecesarios que llevan a un costo adicional.

La consideración de documentos con requisitos de la seguridad similares cuando se asignan los niveles de clasificación puede ser útil para simplificar la labor de clasificación.

En términos generales, la clasificación que se da a la información es una manera corta de determinar la forma en que se debe manejar y proteger esta información.

*(Continúa)*

### *7.2.2 Etiquetado y manejo de la información*

*Control*
Se debería desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.

*Guía de implementación*
Es necesario que los procedimientos para el etiquetado de la información comprendan los activos de información en formatos físico y electrónico.

Las salidas de los sistemas que contienen información que se clasifica como sensible o crítica deberían portar una etiqueta de clasificación adecuada (en la salida). El etiquetado debería reflejar la clasificación según las reglas establecidas en el numeral 7.2.1. Los elementos a considerar incluyen informes impresos, presentaciones en pantalla, medios grabados (por ejemplo, cintas, discos, discos compactos), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción seguros. Ello debería incluir los procedimientos para la cadena de custodia y el registro de cualquier evento importante de la seguridad.

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

*Información adicional*
El etiquetado y el manejo seguro de la información clasificada son un requisito clave de los acuerdos para compartir información. Las etiquetas físicas son una forma común de etiquetado.

No obstante, algunos activos de información, tales como los documentos en formato electrónico, no se pueden identificar físicamente y es necesario emplear medios electrónicos de etiquetado. Por ejemplo, el etiquetado de notificación puede aparecer en la pantalla o en la presentación. Cuando el etiquetado no es viable, se pueden aplicar otros medios para designar la clasificación de la información, por ejemplo a través de procedimientos o meta-datos.

## 8. Seguridad de los recursos humanos

### 8.1 Previo a la contratación laboral [3)]

Objetivo: asegurar que los empleados, contratistas y usuarios de terceras partes entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral, describiendo adecuadamente el trabajo y los términos y condiciones del mismo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para trabajos sensibles.

Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de información deberían firmar un acuerdo sobre sus funciones y responsabilidades de la seguridad.

[3] Explicación: La palabra “contratación" cubre todas las siguientes situaciones: empleo de personas (temporal o a término indefinido), asignación de roles de trabajo, cambio de roles de trabajo, asignación de contratos, y la terminación de cualquiera de estos acuerdos.

*(Continúa)*

***8.1.1 Funciones y responsabilidades***

*Control*
Se deberían definir y documentar los funciones y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de la seguridad de la información de la organización.

*Guía de implementación*
Las funciones y responsabilidades deberían incluir los requisitos para:

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

b) proteger los activos contra acceso, divulgación, modificación, destrucción o interferencia no autorizados;

c) ejecutar procesos o actividades particulares de la seguridad;

d) garantizar que se asigna la responsabilidad a la persona para que tome las acciones;

e) informar los eventos de la seguridad, los eventos potenciales u otros riesgos de la seguridad para la organización.

Las funciones y responsabilidades de la seguridad se deberían definir y comunicar claramente a los candidatos al trabajo durante el proceso previo a su contratación.

*Información adicional*
Se pueden utilizar las descripciones del trabajo para documentar las funciones y responsabilidades para la seguridad. También se deberían definir y comunicar claramente las funciones y responsabilidades para la seguridad de personas no contratadas a través del proceso de contratación de la organización, por ejemplo las contratadas a través de de la organización de tercera parte.

***8.1.2 Selección***

*Control*
Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

*Guía de implementación*
En las revisiones de verificación se deberían tener en cuenta la legislación pertinente a la privacidad, la protección de datos personales y / o el empleo y, cuando se permite, debería incluir lo siguiente:

a) disponibilidad de referencias de comportamiento satisfactorio, por ejemplo una laboral y otra personal;

b) una verificación (para determinar la totalidad y exactitud) de la hoja de vida del candidato;

c) confirmación de las calificaciones profesionales y académicas declaradas;

d) verificación de la identidad (pasaporte o documento similar);

e) verificación de los detalles adicionales tales como créditos o antecedentes criminales.

Cuando un trabajo, bien sea por designación inicial o por promoción, implica que la persona tenga acceso a los servicios de procesamiento de la información y, en particular, si en ellas se maneja información sensible, como por ejemplo información financiera o de alta confidencialidad, la organización debería considerar verificaciones adicionales más detalladas.

Los procedimientos deberían definir los criterios y las limitaciones para las revisiones de verificación, por ejemplo quién es elegible para seleccionar al personal y cómo, cuándo y por qué se realizan las verificaciones.

*(Continúa)*

También deberían llevar a cabo un proceso de selección para los contratistas y los usuarios de terceras partes. Cuando los contratistas son suministrados por una agencia, el contrato con la agencia debería especificar claramente las responsabilidades de la agencia para la selección y los procedimientos de notificación que es necesario seguir si la selección no se ha completado o si los resultados arrojan dudas o preocupación. De la misma manera, el acuerdo con la tercera parte (véase el numeral 6.2.3) debería especificar claramente todas las responsabilidades y los procedimientos de notificación para la selección.

La información sobre todos los candidatos que se consideran para los cargos dentro de la organización se debería recolectar y manejar según la legislación adecuada existente en la jurisdicción correspondiente. Dependiendo de la legislación que se aplique, se debería informar con anticipación a los candidatos sobre las actividades de selección.

### *8.1.3 Términos y condiciones laborales*

*Control*
Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

*Guía de implementación*
Los términos y condiciones laborales deberían reflejar la política de la seguridad de la organización, además debería aclarar y establecer:

a) que todos los empleados, contratistas y usuarios de terceras partes que tengan acceso a información sensible deberían firmar un acuerdo de confidencialidad o no-divulgación antes de tener acceso a los servicios de procesamiento de información;

b) los derechos y responsabilidades legales de los empleados, los contratistas y cualquier otro usuario, por ejemplo con respecto a las leyes de derechos de copia o la legislación sobre protección de datos (véanse los numerales 15.1.1 y 15.1.2);

c) responsabilidades para la clasificación de la información y la gestión de los activos asociados con sistemas y servicios de información manejados por el empleado, el contratista o el usuario de tercer aparte (véanse los numerales 7.2.1 y 10.7.3);

d) responsabilidades del empleado, el contratista o el usuario de tercera parte para el manejo de la información recibida de otras empresas o de partes externas;

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

f) responsabilidades que van más allá de las instalaciones de la organización y de las horas laborales, por ejemplo en el caso de trabajo en el domicilio (véanse los numerales 9.2.5 y 11.7.1);

g) acciones a tomar si el empleado, el contratista o el usuario de tercera parte hace caso omiso de requisitos de la seguridad de la organización (véase el numeral 8.2.3).

La organización debería garantizar que los empleados, los contratistas y los usuarios de terceras partes están de acuerdo con los términos y las condiciones respecto a la seguridad de la información según la naturaleza del acceso que tendrán a los activos de la organización asociados con los sistemas y servicios de información.

Cuando sea apropiado, las responsabilidades contenidas en los términos y condiciones laborales deberían continuar durante un periodo definido después de la terminación del contrato laboral (véase el numeral 8.3)

*(Continúa)*

*Información adicional*
Se puede utilizar un código de conducta que cubra las responsabilidades de los empleados, contratistas y usuarios de terceras partes con relación a la confidencialidad, la protección de datos, la ética, el uso adecuado de las instalaciones y los equipos de la organización, así como las prácticas acreditadas confiables esperadas por la organización. El contratista o los usuarios de terceras partes se pueden asociar con la organización externa a la cual, a su vez, se le puede exigir acuerdos contractuales a nombre de la persona contratada.

## 8.2 Durante la vigencia del contrato laboral

**Objetivo:** asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de la seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

Es conveniente definir las responsabilidades de la dirección para garantizar que se aplica la seguridad durante todo el contrato laboral de una persona dentro de la organización.

Se debería brindar un nivel adecuado de concienciación, educación y formación en los procedimientos de la seguridad y el uso correcto de los servicios de procesamiento de información a todos los empleados, contratistas y usuarios de terceras partes para minimizar los posibles riesgos de la seguridad. Es conveniente establecer un proceso disciplinario formal para el manejo de las violaciones de la seguridad.

### *8.2.1 Responsabilidades de la dirección*

*Control*
La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización.

*Guía de implementación*
Las responsabilidades de la dirección deberían incluir el garantizar que los empleados, los contratistas y los usuarios de terceras partes:

a) estén adecuadamente informados sobre las funciones y las responsabilidades respecto a la seguridad de la información antes de que se les otorgue acceso a información o sistemas de información sensibles;

b) tengan las directrices para establecer las expectativas de la seguridad de sus funciones dentro de la organización;

c) estén motivados para cumplir las políticas de la seguridad de la organización;

d) logren un grado de concienciación sobre la seguridad correspondiente a sus funciones y responsabilidades dentro de la organización (véase el numeral 8.2.2);

e) estén de acuerdo con los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la organización y los métodos apropiados de trabajo;

f) sigan teniendo las calificaciones y las habilidades apropiadas.

*Información adicional*
Si los empleados, contratistas y usuarios de terceras partes no están concientes de sus responsabilidades, pueden causar un daño considerable a la organización. Es probable que el personal motivado sea más confiable y cause menos incidentes de la seguridad de la información.

Una gestión pobre puede hacer que el personal se sienta subvalorado lo que produce un impacto negativo en la seguridad para la organización. Por ejemplo, la gestión pobre puede llevar a que se ignore la seguridad o al uso potencial inadecuado de los activos de la organización.

*(Continúa)*

### *8.2.2 Educación, formación y concienciación sobre la seguridad de la información*

*Control*
Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir formación adecuada en concienciación y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.

*Guía de implementación*
La formación en concienciación debería empezar con un proceso formal de introducción diseñado para presentar las políticas de la seguridad de la organización y las expectativas antes de otorgar el acceso a la información o los servicios.

Es recomendable que la formación continua incluya los requisitos de la seguridad, las responsabilidades legales y los controles del negocio, así como la formación en el uso correcto de los servicios de procesamiento de información como por ejemplo el procedimiento de registro de inicio, el uso de paquetes de software y la información sobre el proceso disciplinario (véase el numeral 8.2.3).

*Información adicional*
Las actividades de concienciación, educación y formación sobre seguridad deberían ser convenientes y pertinentes a la función, las responsabilidades y las habilidades de la persona y deberían incluir información sobre las amenazas conocidas, a quién contactar para obtener asesoría adicional sobre seguridad y los canales apropiados para reportar los incidentes de la seguridad de la información (véase el numeral 13.1).

La formación para promover la concienciación tiene como objetivo permitir que los individuos reconozcan los problemas e incidentes de la seguridad de la información y respondan de acuerdo con las necesidades de su función de trabajo.

### *8.2.3 Proceso disciplinario*

*Control*
Debería existir un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad.

*Guía de implementación*
No se recomienda iniciar el proceso disciplinario antes de verificar que se ha presentado la violación de la seguridad (véase el numeral 13.2.3 para la recolección de evidencia).

El proceso disciplinario formal debería garantizar el tratamiento imparcial y correcto para los empleados de quienes se sospecha han cometido violaciones de la seguridad. El proceso disciplinario formal debería brindar una respuesta gradual que considere factores tales como la naturaleza y la gravedad de la violación y su impacto en el negocio, si es la primera ofensa o se repite, si el violador estaba capacitado adecuadamente, la legislación correspondiente, los contratos de negocios y otros factores, según el caso. En los casos graves de mala conducta el proceso debería permitir el retiro instantáneo de las funciones, los derechos de acceso y los privilegios y el acompañamiento inmediato fuera de las instalaciones, si es necesario.

*Información adicional*
El proceso disciplinario también se debería utilizar como disuasión para evitar que los empleados, los contratistas y los usuarios de terceras partes violen las políticas y los procedimientos de la seguridad de la organización, así como para cualquier otra violación de la seguridad.

*(Continúa)*

## 8.3 Terminación o cambio de la contratación laboral

**Objetivo:** asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.

Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que se completa la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

Los cambios en las responsabilidades y las relaciones laborales dentro de la organización se deberían gestionar como la terminación de la respectiva responsabilidad o contrato laboral según esta sección y todos las contrataciones nuevas se deberían gestionar como se describe en el numeral 8.1.

### *8.3.1 Responsabilidades en la terminación del contrato*

*Control*
Se deberían definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.

*Guía de implementación*
La comunicación de las responsabilidades en la terminación debería incluir los requisitos permanentes de la seguridad y las responsabilidades legales y, cuando sea apropiado, las responsabilidades contenidas en cualquier acuerdo de confidencialidad (véase el numeral 6.1.5), y los términos y condiciones laborales (véase el numeral 8.1.3) deberían continuar durante un periodo definido después de terminar la contratación laboral del empleado, el contratista o el usuario de terceras partes.

Los contratos del empleado, el contratista o el usuario de terceras partes deberían incluir las responsabilidades y deberes válidos aún después de la terminación del contrato laboral.

Los cambios en la responsabilidad o en el contrato laboral deberían ser gestionados como la terminación de la responsabilidad o el contrato laboral respectivo, y la nueva responsabilidad o contrato laboral se debería controlar tal como se describe en el numeral 8.1.

*Información adicional*
Por lo general, la función de recursos humanos es responsable del proceso total de terminación y actúa junto con el director supervisor de la persona que se retira, para gestionar los aspectos de la seguridad de los procedimientos pertinentes. En el caso de un contratista, este proceso de responsabilidad en la terminación puede ser realizado por la agencia responsable del contratista y en el caso de otro usuario puede ser manejado por su organización.

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

### *8.3.2 Devolución de activos*

*Control*
Todos los empleados, contratistas o usuarios de terceras partes deberían devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.

*Guía de implementación*
Se debería formalizar el proceso de terminación para incluir la devolución del software previamente publicado, los documentos corporativos y los equipos. También es necesaria la devolución de otros activos de la organización tales como los dispositivos de cómputo móviles, las tarjetas de crédito, las tarjetas de acceso, el software, los manuales y la información almacenada en medios electrónicos.

*(Continúa)*

Cuando un empleado, contratista o usuario de terceras partes adquiere equipo de la organización o utiliza su propio equipo, se deberían seguir los procedimientos para garantizar que toda la información pertinente se transfiere a la organización y se elimina con seguridad de tal equipo (véase el numeral 10.7.1).

Cuando un empleado, contratista o usuario de terceras partes tiene un conocimiento que es importante para la continuación de las operaciones, esa información debería estar documentada y transferirse a la organización.

***8.3.3 Retiro de los derechos de acceso***

*Control*
Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deberían retirar al finalizar su contratación laboral, contrato o acuerdo o se deberían ajustar después del cambio.

*Guía de implementación*
Después de la terminación, se deberían reconsiderar los derechos de acceso de la persona a los activos asociados con los sistemas y servicios de información. Ello determinará si es necesario retirar los derechos de acceso. Los cambios en un cargo se deberían reflejar en el retiro de todos los derechos de acceso que no estén aprobados para el nuevo cargo. Los derechos de acceso que se deberían adaptar o retirar incluyen acceso físico y lógico, claves, tarjetas de identificación, servicios de procesamiento de información (véase el numeral 11.2.4), suscripciones y retiro de cualquier documentación que lo identifique como miembro actual de la organización. Si un empleado, contratista o usuario de terceras partes que se retira tiene contraseñas conocidas para permanecer activo, éstas se deberían cambiar en la terminación o el cambio de empleo, contrato o acuerdo.

Los derechos de acceso a los activos de información y a los servicios de procesamiento de información se deberían reducir o retirar antes de la finalización o cambio del contrato laboral, dependiendo de una evaluación de factores de riesgo tales como:

a) si la terminación o el cambio es iniciativa del empleado, contratista o usuario de terceras partes o por la dirección y el motivo de dicha terminación;

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

c) el valor de los activos actualmente accesibles.

*Información adicional*
En algunas circunstancias los derechos de acceso se pueden asignar con base en la disponibilidad para otras personas diferentes al empleado, contratista o usuario de terceras partes que se retira, por ejemplo las identificaciones de usuario para grupo. En dichas circunstancias, las personas que se retiran se deberían eliminar de todas las listas de acceso de grupo y se deberían formular acuerdos para notificar a los otros empleados, contratistas o usuarios de terceras partes involucrados que ya no compartirán esta información con la persona que se retira.

En los casos de terminación iniciada por la dirección, los empleados, contratistas o usuarios de terceras partes descontentos pueden corromper deliberadamente la información o sabotear los servicios de procesamiento de información. En el caso de las personas que renuncian, ellas pueden intentar recolectar información para uso futuro.

*(Continúa)*

# 9. Seguridad física y del entorno

## 9.1 Áreas seguras

Objetivo: evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Los servicios de procesamiento de información sensible o crítica deberían estar ubicados en áreas seguras, protegidas por perímetros de la seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia.

La protección suministrada debería estar acorde con los riesgos identificados.

### *9.1.1 Perímetro de la seguridad física*

*Control*
Se deberían utilizar perímetros de la seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.

*Guía de implementación*
Se deberían considerar e implementar las siguientes directrices para los perímetros de la seguridad física:

a) se recomienda definir claramente los perímetros de la seguridad y la ubicación y la fortaleza de cada perímetro deberían depender de los requisitos de la seguridad de los activos dentro del perímetro, así como de los resultados de una evaluación de riesgos;

b) los perímetros de una edificación o un lugar que contenga servicios de procesamiento de información deberían ser robustos físicamente (es decir, no deberían existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir una intrusión); las paredes externas del sitio deberían tener una construcción sólida y todas las puertas externas deberían tener protección adecuada contra el acceso no autorizado con mecanismos de control tales como barras, alarmas, relojes, etc., las puertas y ventanas deberían estar cerradas con llave cuando no están atendidas y se debería tener presente la protección externa para las ventanas, particularmente a nivel del suelo;

c) se debería establecer un área de recepción con personal u otros medios para controlar el acceso físico al lugar o edificación; el acceso a los sitios y edificaciones debería estar restringido únicamente al personal autorizado;

d) cuando sea viable, se deberían construir barreras físicas para evitar el acceso físico no autorizado y la contaminación ambiental;

e) todas las puertas de incendio en el perímetro de la seguridad deberían tener alarma, monitorearse y someterse a prueba junto con las paredes para establecer el grado requerido de resistencia, según las normas regionales, nacionales e internacionales; éstas deberían funcionar de manera segura de acuerdo con el código local de incendios;

f) es recomendable la instalación de sistemas adecuados de detección de intrusos según normas nacionales, regionales o internacionales y someterlos a pruebas regularmente para verificar todas las puertas externas y ventanas accesibles; las áreas desocupadas siempre deberían tener alarmas, también se debería tener cubrimiento de otras áreas, por ejemplo los recintos de computadores o de comunicaciones;

g) los servicios de procesamiento de información dirigidos por la organización deberían estar físicamente separados de aquellos dirigidos por terceras partes.

*(Continúa)*

*Información adicional*
La protección física se puede lograr creando una o más barreras físicas alrededor de las instalaciones y los servicios de procesamiento de información de la organización. El empleo de barreras múltiples proporciona protección adicional, cuando la falla de una sola barrera no implica que la seguridad se vea comprometida inmediatamente.

Un área segura puede ser una oficina que se pueda asegurar o varios recintos rodeados por continuas barreras de la seguridad física internas. Pueden ser necesarias las barreras y los perímetros adicionales para controlar el acceso físico entre áreas con requisitos de la seguridad diferentes dentro del perímetro de la seguridad.

Se debería considerar especialmente la seguridad del acceso físico a las edificaciones en donde se encuentran varias organizaciones.

***9.1.2 Controles de acceso físico***

*Control*
Las áreas seguras deberían estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

*Guía de implementación*
Se deberían tener en cuenta las siguientes directrices:

a) se deberían registrar la fecha y la hora de entrada y salida de visitantes y todos los visitantes deberían estar supervisados, a menos que su acceso haya sido aprobado previamente; sólo se les debería dar acceso para propósitos específicos y autorizados y dicho acceso se debería emitir con instrucciones sobre los requisitos de la seguridad del área y sobre los procedimientos de emergencia;

b) se debería controlar el acceso a áreas en donde se procesa o almacena información sensible y restringir el acceso únicamente a personas autorizadas; se deberían utilizar controles de autenticación como las tarjetas de control de acceso más el número de identificación personal (PIN) para autorizar y validar el acceso, se recomienda mantener de forma segura una prueba de auditoría de todos los accesos;

c) se debería exigir a todos los empleados, contratistas y usuarios de terceras partes la utilización de alguna forma de identificación visible y se debería notificar inmediatamente al personal de la seguridad si se encuentran visitantes sin acompañante y cualquiera que no use identificación visible;

d) al personal del servicio de soporte de terceras partes se le debería dar acceso restringido a las áreas seguras o a los servicios de procesamiento de información sensible únicamente cuando sea necesario; éste acceso se debería autorizar y monitorear;

e) los derechos de acceso a áreas seguras se deberían revisar y actualizar con regularidad y revocados cuando sea necesario (véase el numeral 8.3.3).

***9.1.3 Seguridad de oficinas, recintos e instalaciones***

*Control*
Se debería diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.

*Guía de implementación*
Se recomienda tener en cuenta las siguientes directrices para la seguridad de oficinas, recintos y servicios:

a) tener presente los reglamentos y las normas pertinentes a la seguridad y la salud;

b) las instalaciones claves se deberían ubicar de modo que se evite el acceso al público;

*(Continúa)*

c) cuando sea viable, las edificaciones deberían ser discretas y no tener indicaciones sobre su propósito, sin señales obvias, fuera o dentro de ellas, que identifiquen la presencia de actividades de procesamiento de información;

d) los directorios y los listados telefónicos internos que indican las ubicaciones de los servicios de procesamiento de información sensible no deberían ser de fácil acceso al público.

***9.1.4 Protección contra amenazas externas y ambientales***

*Control*
Se deberían diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

*Guía de implementación*
Se deben tener en cuenta todas las amenazas para la seguridad que presentan las instalaciones circundantes, por ejemplo, un incendio en la edificación contigua, fuga de agua por un techo o en los pisos por debajo del nivel del suelo o una explosión en la calle.

Se recomienda tener en mente las siguientes directrices para evitar daño debido a incendio, inundación, terremoto, explosión, malestar social, y otras formas de desastre natural o artificial:

a) los materiales combustibles o peligrosos se deberían almacenar a una distancia prudente del área de la seguridad. Los suministros a granel tales como los materiales de oficina, no se deberían almacenar en un área segura;

b) los equipos de repuesto y los medios de soporte de la seguridad se deberían ubicar a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales;

c) se debería suministrar equipo apropiado contra incendios y ubicarlo adecuadamente.

***9.1.5 Trabajo en áreas seguras***

*Control*
Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

*Guía de implementación*
Se deberían considerar las siguientes directrices:

a) el personal sólo debería conocer la existencia de un área segura o las actividades dentro de ella en función de la necesidad con base conocida;

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

c) las áreas seguras vacías deberían tener bloqueo físico y se deberían revisar periódicamente;

d) no se debería permitir equipo de grabación fotográfica, de video, de audio ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.

Las disposiciones para el trabajo en áreas seguras incluyen controles para los empleados, contratistas y usuarios de terceras partes que laboran en el área segura, así como otras actividades de tercera parte que tengan lugar.

***9.1.6 Áreas de carga, despacho y acceso público***

*Control*
Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

*(Continúa)*

*Guía de implementación*
Se recomienda considerar las siguientes directrices

a) se debería restringir el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado;

b) el área de despacho y carga se debería designar de forma tal que los suministros se puedan descargar sin que el personal de despacho tenga acceso a otras partes de la edificación;

c) las puertas externas del área de despacho y entrega deberían estar aseguradas mientras las puertas internas estén abiertas;

d) el material que llega se debería inspeccionar para determinar posibles amenazas (véase el numeral 9.2.1d) antes de moverlo desde el área de despacho y carga hasta el punto de uso;

e) el material que llega se debería registrar de acuerdo con los procedimientos de gestión de activos (véase el numeral 7.1.1) a su entrada al lugar;

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

## 9.2 Seguridad de los equipos

Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

Los equipos deberían estar protegidos contra amenazas físicas y ambientales.

La protección del equipo (incluyendo el utilizado externamente y el retirado de la propiedad) es necesaria para reducir el riesgo de acceso no autorizado a la información y para proteger contra pérdida o daño. También se debería considerar la ubicación y la eliminación de los equipos. Es posible que se requieran controles especiales para la protección contra amenazas físicas y para salvaguardar los servicios de soporte tales como energía eléctrica e infraestructura de cableado.

### *9.2.1 Ubicación y protección de los equipos*

*Control*
Los equipos deberían estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.

*Guía de implementación*
Se recomienda considerar las siguientes directrices para la protección de los equipos:

a) Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo;

b) los servicios de procesamiento de información que manejan datos sensibles, deberían estar ubicados de forma tal que se reduzca el riesgo de visualización de la información por personas no autorizadas durante su uso, y los sitios de almacenamiento se deberían asegurar para evitar el acceso no autorizado;

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

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

e) se deberían establecer directrices para comer, beber y fumar en las cercanías de los servicios de procesamiento de información;

*(Continúa)*

f) es conveniente monitorear las condiciones ambientales, como temperatura y humedad, para determinar las condiciones que podrían afectar adversamente el funcionamiento de los servicios de procesamiento de información;

g) se debería aplicar protección contra rayos a todas las edificaciones y adaptar filtros protectores a las fuentes de energía entrantes y a las líneas de comunicación;

h) es recomendable considerar la utilización de métodos especiales de protección para equipos en ambientes industriales, tales como membranas para los teclados;

i) Los equipos de procesamiento de información sensible deberían estar protegidos para minimizar el riesgo de fuga de información debido a filtración.

***9.2.2 Servicios de suministro***

*Control*
Los equipos deberían estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.

*Guía de implementación*
Todos los servicios de suministro, tales como electricidad, agua, alcantarillado, calefacción /ventilación y aire acondicionado deberían ser adecuados para los sistemas a los que dan apoyo. Los servicios de suministro se deberían inspeccionar regularmente y someter a las pruebas apropiadas para garantizar su funcionamiento adecuado y reducir cualquier riesgo debido a su mal funcionamiento o falla. Se recomienda proporcionar un suministro eléctrico acorde con las especificaciones del fabricante del equipo.

Se recomienda el suministro de energía sin interrupción (UPS) para dar soporte al cierre ordenado o al funcionamiento continuo de equipos que soportan operaciones críticas para el negocio. Los planes de contingencia deberían incluir la acción que se ha de tomar en caso de falla de la UPS. Se recomienda pensar en una planta de energía alterna, si se requiere la continuidad del procesamiento en caso de fallas energéticas prolongadas.

Debería estar disponible un suministro adecuado de combustible para garantizar que el generador pueda funcionar por un periodo prolongado. El equipo de UPS y los generadores se deberían revisar con regularidad para asegurarse de que tienen la capacidad adecuada y someterse a prueba según las recomendaciones del fabricante.

Además, se debe estudiar el uso de fuentes múltiples de energía o, si el lugar es grande, una subestación de energía independiente.

Los interruptores de emergencia para apagar la energía deberían estar cerca de las salidas de emergencia en los recintos de los equipos para facilitar el corte rápido de energía en caso de emergencia. Se recomienda tener iluminación de emergencia en caso de falla del suministro principal.

El suministro de agua debería ser estable y adecuado para alimentar el aire acondicionado, el equipo de humidificación y los sistemas de extinción de incendios (cuando se utilizan). El funcionamiento inadecuado en el sistema de suministro de agua puede dañar el equipo o evitar la acción eficaz de la extinción de incendios. Se debería valorar e instalar, si se requiere, un sistema de alarma para detectar el funcionamiento inadecuado en los servicios de soporte.

El equipo de telecomunicaciones se debería conectar al proveedor del servicio mediante al menos dos rutas diferentes para evitar que la falla en una ruta de conexión elimine los servicios de voz. Estos servicios deberían ser adecuados para satisfacer los requisitos legales locales para comunicaciones de emergencia.

*Información adicional*

Las opciones para lograr la continuidad del suministro de energía incluyen fuentes de alimentación múltiples para evitar un solo punto de falla en el suministro de energía.

*(Continúa)*

***9.2.3 Seguridad del cableado***

*Control*
El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deberían estar protegidos contra interceptaciones o daños.

*Guía de implementación*
Se recomienda tener en cuenta las siguientes directrices para la seguridad del cableado:

a) las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada;

b) el cableado de la red debería estar protegido contra interceptación no autorizada o daño, por ejemplo utilizando conductos o evitando rutas a través de áreas públicas;

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

d) se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones accidentales de cables erróneos a la red;

e) es recomendable emplear un plano del cableado para reducir la posibilidad de errores;

f) para sistemas críticos o sensibles considerar controles adicionales incluyendo:

1) instalación de conductos blindados y recintos o cajas bloqueadas en los puntos de inspección y terminación;

2) uso de medios alternos de enrutamiento y / o transmisión que suministren seguridad adecuada;

3) uso de cableado de fibra óptica;

4) uso de cubiertas (blindaje) electromagnéticas para proteger los cables;

5) inicio de reconocimientos técnicos e inspecciones físicas en busca de dispositivos no autorizados conectados al cableado;

6) acceso controlado a los módulos de cableado (patch panel) y a cuartos de cableado.

***9.2.4 Mantenimiento de los equipos***

*Control*
Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

*Guía de implementación*
Se recomienda considerar las siguientes directrices para el mantenimiento de los equipos:

a) el mantenimiento de los equipos debería estar acorde con las especificaciones y los intervalos de servicio recomendados por el proveedor;

b) sólo personal de mantenimiento autorizado debería realizar las reparaciones y el servicio de los equipos;

c) se recomienda conservar registros de todas las fallas reales o sospechadas y de todo el mantenimiento preventivo y correctivo;

d) es recomendable implementar controles apropiados cuando se programa el mantenimiento para los equipos, teniendo en cuenta si el mantenimiento lo realiza el personal dentro o fuera de la organización; cuando sea necesario, la información sensible se debería retirar del entorno del equipo o el personal de mantenimiento debería ser suficientemente revisado;

*(Continúa)*

e) se deberían cumplir todos los requisitos impuestos por las pólizas de seguros.

### *9.2.5 Seguridad de los equipos fuera de las instalaciones*

*Control*
Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

*Guía de implementación*
Independientemente del responsable, la dirección debería autorizar el uso del equipo de procesamiento de información fuera de las instalaciones de la organización.

Se recomienda tener en cuenta las siguientes directrices para la protección del equipo fuera de las instalaciones:

a) el equipo y los medios llevados fuera de las instalaciones no se deberían dejar solos en sitios públicos, los computadores portátiles se deberían llevar como equipaje de mano y camuflado, cuando sea posible, durante los viajes;

b) se deberían observar en todo momento las instrucciones del fabricante para la protección del equipo, por ejemplo, protección contra la exposición a campos electromagnéticos fuertes;

c) se recomienda determinar controles para el trabajo que se realiza en casa mediante una evaluación de riesgos y controles adecuados que se aplican de forma idónea, por ejemplo gabinetes de archivos con seguro, política de escritorio despejado, controles de acceso a los computadores y comunicaciones seguras con la oficina (véase la norma ISO/IEC 18028, Seguridad de la red);

d) se debería establecer la cobertura adecuada del seguro, para proteger el equipo fuera de las instalaciones.

Los riesgos de la seguridad, como daño, robo o escuchas no autorizadas pueden variar considerablemente entre los lugares y se deberían tener en cuenta para determinar los controles más apropiados.

*Información adicional*
El almacenamiento de información y el equipo de procesamiento incluyen todas las formas de computadores personales, organizadores, teléfonos móviles, tarjetas electrónicas, papel u otras formas que se conservan para el trabajo en el domicilio o que se transportan lejos del sitio normal de trabajo.

Información adicional sobre otros aspectos de la protección de equipo móvil se puede encontrar en el numeral 11.7.1.

### *9.2.6 Seguridad en la reutilización o eliminación de los equipos*

*Control*
Se deberían verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.

*Guía de implementación*
Los dispositivos que contienen información sensible se deberían destruir físicamente o su información se debería destruir, borrar o sobrescribir usando técnicas que permitan que la información original no se pueda recuperar, en lugar de utilizar las funciones de borrado o formateado estándar.

*Información adicional*
Los dispositivos deteriorados que contengan datos sensibles pueden requerir una evaluación de riesgos para determinar si los elementos se deberían destruir físicamente en lugar de enviarlos a reparación o desecharlos.

*(Continúa)*

La información se puede poner en peligro con la eliminación descuidada o la reutilización del equipo (véase el numeral 10.7.2).

***9.2.7 Retiro de activos de la propiedad***

*Control*
Ningún equipo, información ni software se deberían retirar sin autorización previa.

*Guía de implementación*
Se recomienda tener presentes las siguientes directrices:

a) ni los equipos, ni la información, tampoco el software se deberían retirar sin autorización previa;

b) los empleados, contratistas y usuarios de terceras partes que tengan autoridad para permitir retirar activos deberían estar claramente identificados;

c) se recomienda establecer límites de tiempo para el retiro de equipos y verificar el cumplimiento en el momento de devolución;

d) cuando sea necesario y adecuado, se debería registrar que el equipo ha sido retirado y se debe registrar cuando fue devuelto.

*Información adicional*
Los controles al azar, realizados para determinar el retiro no autorizado de propiedad, también se pueden usar para detectar dispositivos de grabación no autorizados, armas, etc., y evitar su ingreso. Tales controles al azar se deberían llevar a cabo según la legislación y los reglamentos pertinentes. Las personas deberían saber si se realizan controles al azar y éstos se deberían ejecutar con la autorización adecuada para los requisitos legales y reglamentarios.

## 10. Gestión de comunicaciones y operaciones

### 10.1 Procedimientos operacionales y responsabilidades

Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.

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

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

***10.1.1 Documentación de los procedimientos de operación***

*Control*
Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

*Guía de implementación*
Se deberían elaborar procedimientos documentados para las actividades del sistema asociadas con los servicios de comunicaciones y de procesamiento de información, como por ejemplo procedimientos para el encendido y apagado de los computadores, copias de respaldo, mantenimiento de equipos, manejo de los medios, cuarto de equipos y gestión del correo, como también de la seguridad.

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

*(Continúa)*

a) procesamiento y manejo de información;

b) copias de respaldo (véase el numeral 10.5);

c) requisitos de programación, incluyendo las interrelaciones con otros sistemas, hora de comienzo de la tarea inicial y de terminación de la tarea final;

d) instrucciones para el manejo de errores y otras condiciones excepcionales que se pueden presentar durante la ejecución del trabajo, incluyendo las restricciones al uso de las utilidades del sistema (véase el numeral 11.5.4);

e) contactos de soporte en caso de dificultades técnicas u operativas inesperadas;

f) Instrucciones de manejo de los medios y los informes especiales, como el uso de papelería especial o el manejo de los informes confidenciales incluyendo los procedimientos para la eliminación segura de los informes de tareas fallidas (véanse los numerales 10.7.2 y 10.7.3);

g) procedimientos para el reinicio y la recuperación del sistema que se han de usar en caso de falla del sistema;

h) gestión de los registros de auditoria y de la información de registro del sistema (véase el numeral 10.10).

Los procedimientos operativos, y los procedimientos documentados para las actividades del sistema, se deberían tratar como documentos formales y sus cambios deberían ser autorizados por la dirección. Cuando sea técnicamente viable, se recomienda gestionar los sistemas de información de forma consistente, utilizando los mismos procedimientos, herramientas y utilidades.

***10.1.2 Gestión del cambio***

*Control*
Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

*Guía de implementación*
Los sistemas operativos y el software de aplicación deberían estar sujetos a un control estricto de la gestión del cambio.

En particular, se deberían considerar los siguientes elementos:

a) identificación y registro de los cambios significativos;

b) planificación y pruebas de los cambios;

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

d) procedimiento de aprobación formal para los cambios propuestos;

e) comunicación de los detalles del cambio a todas las personas implicadas;

f) procedimientos de emergencia, incluyendo los procedimientos y las responsabilidades de cancelar o recuperarse de cambios fallidos y eventos imprevistos.

Se deberían establecer las responsabilidades y los procedimientos formales de gestión para garantizar el control satisfactorio de todos los cambios en los equipos, el software o los procedimientos. Cuando se realicen los cambios, es conveniente conservar un registro de auditoría que contenga toda la información pertinente.

*Información adicional*
El control inadecuado de los cambios en los sistemas y los servicios de procesamiento de información es una causa común de falla del sistema o de la seguridad. Los cambios en el entorno operativo, especialmente cuando se transfiere un sistema de la fase de desarrollo a la operativa puede tener impacto en la confiabilidad de las aplicaciones (véase el numeral 12.5.1).

*(Continúa)*

Los cambios en los sistemas operativos sólo se deberían realizar cuando existe una razón válida para el negocio, como por ejemplo un aumento en el riesgo para el sistema. La actualización de los sistemas con las últimas versiones del sistema operativo o de la aplicación no siempre favorece el interés del negocio y ello podría introducir más vulnerabilidades e inestabilidad que la versión vigente. También puede existir la necesidad de formación adicional, costos de licencias, soporte, costos generales de mantenimiento y administración y nuevo hardware, especialmente durante la migración.

***10.1.3 Distribución de funciones***

*Control*
Las funciones y las áreas de responsabilidad se deberían distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

*Guía de implementación*
La distribución de funciones es un método para reducir el riesgo de uso inadecuado deliberado o accidental del sistema. Se debería tener cuidado de que ninguna persona pueda tener acceso, modificar o utilizar los activos sin autorización o sin ser detectado. La iniciación de un evento se debería separar de su autorización. Es conveniente considerar la posibilidad de complicidad al diseñar los controles.

Las organizaciones pequeñas pueden encontrar difícil de lograr la distribución de funciones, pero el principio se debería aplicar en la medida de lo posible y viable. Cuando haya dificultad para la distribución, se deberían considerar otros controles como monitoreo de actividades, registros de auditoría y supervisión por la dirección. Es importante que la auditoría de la seguridad siga siendo independiente.

***10.1.4 Separación de las instalaciones de desarrollo, ensayo y operación***

*Control*
Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

*Guía de implementación*
Se debería identificar el grado de separación entre los ambientes operativo, de prueba y de desarrollo que es necesario para prevenir problemas operativos e implementar los controles adecuados.

Se deberían tener presentes los siguientes elementos:

a) se recomienda definir y documentar las reglas para la transferencia de software del estado de desarrollo al operativo;

b) el software de desarrollo y el operativo se deberían ejecutar en diferentes sistemas o procesadores de computación y en diferentes dominios o directorios;

c) los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberían ser accesibles desde los sistemas operativos cuando no se requiera;

d) el ambiente del sistema de prueba debería emular al ambiente del sistema operativo lo más estrechamente posible;

e) los usuarios deberían emplear perfiles de usuario diferentes para los sistemas operativos y de prueba y los menús deberían desplegar mensajes de identificación adecuados para reducir el riesgo de error;

f) los datos sensibles no se deberían copiar en el entorno del sistema de prueba (véase el numeral 12.4.2).

*Información adicional*
Las actividades de desarrollo y de prueba pueden causar problemas graves, como la modificación indeseada de archivos o del entorno del sistema, o falla del sistema. En este caso, es necesario mantener un entorno conocido y estable en el cual realizar pruebas significativas y evitar el acceso inadecuado de los desarrolladores.

*(Continúa)*

Cuando el personal de desarrollo y de pruebas tiene acceso al sistema operativo y su información, pueden introducir códigos no autorizados y sin probar o alterar los datos operativos. En algunos sistemas, esta capacidad podría ser mal utilizada para cometer fraude o introducir códigos sin probar o maliciosos, lo cual puede crear problemas operativos graves.

Quienes desarrollan y realizan las pruebas imponen una amenaza a la confidencialidad de la información operativa. Las actividades de desarrollo y de prueba pueden causar cambios involuntarios en el software o la información si comparten el mismo entorno de computación.

Por lo tanto, es conveniente separar las instalaciones de desarrollo, de prueba y operativas para reducir el riesgo de cambio accidental o acceso no autorizado al software operativo o a los datos del negocio (véase el numeral 12.4.2 para la protección de los datos de prueba).

## 10.2 Gestión de la prestación del servicio por terceras partes

| |
|---|
| Objetivo: implementar y mantener un grado adecuado de la seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros,<br><br>La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros. |

### *10.2.1 Prestación del servicio*

*Control*
Se deberían garantizar que los controles de la seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por el tercero.

*Guía de implementación*
La prestación de servicios por terceros debería incluir los acuerdos sobre disposiciones de la seguridad, definiciones del servicio y aspectos de la gestión del mismo. En el caso de contrataciones externas, la organización debería planificar las transiciones necesarias (de información, servicios de procesamiento de información y todo lo demás que se deba transferir) y garantizar que la seguridad se mantiene durante todo el periodo de transición.

Es recomendable que la organización garantice que la tercera parte mantenga una capacidad de servicio suficiente, junto con planes ejecutables diseñados para garantizar la conservación de los niveles de continuidad del servicio acordados, después de desastres o fallas significativas en el servicio (véase el numeral 14.1).

### *10.2.2 Monitoreo y revisión de los servicios por terceros*

*Control*
Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares.

*Guía de implementación*
El monitoreo y la revisión de los servicios proporcionados por terceras partes deberían garantizar el cumplimiento de los términos y condiciones de la seguridad de la información, de los acuerdos y que los incidentes y problemas de la seguridad de la información se manejen adecuadamente.

Ello debería implicar una relación y un proceso de gestión del servicio entre la organización y la tercera parte para:

a) monitorear los niveles de desempeño del servicio para verificar el cumplimiento de los acuerdos;

*(Continúa)*

b) revisar los reportes del servicio elaborados por la tercera parte y acordar reuniones periódicas sobre el progreso, según lo exijan los acuerdos;

c) suministrar información sobre los incidentes de la seguridad de la información, y revisión de esta información por parte de la organización y la tercera parte, según lo exijan los acuerdos, directrices y los procedimientos de soporte;

d) revisión de los registros y pruebas de auditoría de la tercera parte con respecto a eventos de la seguridad, problemas operativos, fallas, rastreo de fallas e interrupciones relacionadas con el servicio prestado;

e) resolver y manejar todos los problemas identificados.

La responsabilidad por la gestión de la relación con la tercera parte se le debería asignar a una persona o a un equipo de gestión del servicio. Además, la organización debería garantizar que la tercera parte asigna responsabilidades para la verificación del cumplimiento y la aplicación de los requisitos de los acuerdos. Se recomienda poner a disposición suficientes habilidades técnicas y recursos para monitorear el cumplimiento de los requisitos del acuerdo (véase el numeral 6.2.3), en particular los requisitos de la seguridad de la información. Cuando se observan deficiencias en la prestación del servicio se deberían tomar las acciones adecuadas.

La organización debería mantener suficiente control global y no perder de vista todos los aspectos de la seguridad para la información sensible o crítica, o de los servicios de procesamiento de información que haya procesado, gestionado o tenido acceso la tercera parte. La organización debería asegurarse de que conserva visibilidad en las actividades de la seguridad como gestión de cambios, identificación de vulnerabilidades e informe / respuesta de los incidentes de la seguridad de la información a través de un proceso, estructuras y formatos definidos claramente para la presentación de informes.

*Información adicional*

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

***10.2.3 Gestión de los cambios en los servicios por terceras partes***

*Control*
Los cambios en la prestación de los servicios, incluyendo mantenimiento y mejora de las políticas existentes de la seguridad de la información, en los procedimientos y los controles se deberían gestionar teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos.

*Guía de implementación*
Es necesario que el proceso de gestión de los cambios en el servicio prestado por la tercera parte tome en consideración:

a) los cambios hechos por la organización para implementar:

1) mejoras en los servicios actuales ofrecidos;

2) desarrollo de todos los sistemas o aplicaciones nuevas;

3) modificaciones o actualizaciones de las políticas y procedimientos de la organización;

4) controles nuevos para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;

b) cambios en los servicios por la tercera parte para implementar:

1) cambios y mejoras en las redes;

2) uso de nuevas tecnologías;

*(Continúa)*

3) adopción de productos nuevos o versiones / divulgaciones más recientes;

4) nuevas herramientas y entornos de desarrollo;

5) cambios en la ubicación física de las instalaciones de los servicios;

6) cambio de proveedores.

## 10.3 Planificación y aceptación del sistema

**Objetivo:** minimizar el riesgo de fallas en los sistemas.

Se requieren una previa planificación y preparación para garantizar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño requerido del sistema.

Es necesario hacer proyecciones de la capacidad futura para reducir el riesgo de sobrecarga del sistema.

Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.

### *10.3.1 Gestión de la capacidad*

*Control*
Se debería hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

*Guía de implementación*
Para cada actividad nueva y existente es conveniente identificar los requisitos de la capacidad.

Se recomienda monitorear y adaptar el sistema para garantizar y, cuando sea necesario, mejorar la capacidad y la eficacia de los sistemas. Se deberían establecer controles de indagación para indicar los problemas en el momento oportuno. En las proyecciones de los requisitos de capacidad futura se deberían considerar los negocios nuevos y los requisitos del sistema, así como las tendencias actuales y proyectadas en la capacidad de procesamiento de información de la organización.

Es necesario poner atención a los recursos cuya adquisición toma mucho tiempo o requiere costos elevados; por lo tanto, los directores deberían monitorear la utilización de los recursos claves del sistema. También deberían identificar las tendencias del uso, particularmente en relación con las aplicaciones del negocio o las herramientas del sistema de información para la gestión.

Es conveniente que los directores utilicen esta información para identificar y evitar posibles cuellos de botella así como la dependencia de personal clave, los cuales pueden presentar una amenaza para los servicios o la seguridad del sistema, y para planificar la acción adecuada.

### *10.3.2 Aceptación del sistema*

*Control*
Se deberían establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.

*Guía de implementación*
Los directores deberían garantizar que los requisitos y los criterios para la aceptación de sistemas nuevos están definidos, acordados, documentados y probados claramente. Los sistemas de información nuevos, las actualizaciones y las nuevas versiones únicamente deberían migrar a producción después de obtener la aceptación formal. Se deberían considerar los siguientes elementos antes de la aceptación formal:

*(Continúa)*

a) requisitos de desempeño y capacidad de los computadores;

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

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

d) establecimiento del conjunto de controles de la seguridad acordados;

e) procedimientos manuales eficaces;

f) disposiciones para la continuidad del negocio (véase el numeral 14.1);

g) evidencia de que la instalación del sistema nuevo no afectará adversamente a los sistemas existentes, particularmente en los momentos pico de procesamiento, como al final de mes;

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

i) formación en el funcionamiento o utilización de los sistemas nuevos;

j) facilidad de uso, en la medida en que afecte el desempeño del usuario y evite el error humano.

Para nuevos desarrollos importantes se debería consultar a los usuarios y a la función de operaciones en todas las fases del proceso de desarrollo para garantizar la eficiencia operativa del diseño del sistema propuesto. Es conveniente llevar a cabo pruebas adecuadas para confirmar el cumplimiento pleno de todos los criterios de aceptación.

*Información adicional*
La aceptación puede incluir un proceso formal de certificación y acreditación para verificar que el tratamiento que se ha dado a los requisitos de la seguridad es el adecuado.

## 10.4 Protección contra códigos maliciosos y móviles

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

Se requieren precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados.

El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.

### *10.4.1 Controles contra códigos maliciosos*

*Control*
Se deberían implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concienciación de los usuarios.

*Guía de implementación*
La protección contra códigos maliciosos se debería basar en software de detección y reparación de códigos maliciosos, conciencia sobre seguridad, acceso apropiado al sistema y controles en la gestión de cambios. Se recomienda considerar las siguientes directrices:

a) establecer una política formal que prohíba el uso de software no autorizado (véase el numeral 15.1.2);

*(Continúa)*

b) establecer una política formal para la protección contra los riesgos asociados con la obtención de archivos y software, bien sea desde o a través de redes externas o cualquier otro medio, indicando las medidas de protección que se deberían tomar;

c) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que dan soporte a los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o modificaciones no autorizadas;

d) instalación y actualización regular del software de detección y reparación de códigos maliciosos para explorar los computadores y los medios, como control preventivo o de forma rutinaria; las verificaciones realizadas deberían incluir:

1) verificación de la presencia de códigos maliciosos en todos los archivos en medios ópticos o electrónicos y archivos recibidos en las redes antes de su uso;

2) verificación de la presencia de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso; esta verificación se debería efectuar en diferentes lugares, por ejemplo en los servidores de correo electrónico, los computadores de escritorio y cuando ingresan a la red de la organización;

3) verificación de las páginas web para comprobar la presencia de códigos maliciosos;

e) definir responsabilidades y procedimientos de gestión para tratar la protección contra códigos maliciosos en los sistemas, la formación sobre su uso, el reporte y la recuperación debido a ataques de códigos maliciosos (véanse los numerales 13.1 y 13.2);

f) preparación de planes adecuados para la continuidad del negocio con el fin de recuperarse de los ataques de códigos maliciosos, incluyendo todos los datos y el soporte de software necesario y las disposiciones para la recuperación (véase el numeral 14);

g) implementación de procedimientos para recolectar información con regularidad, como la suscripción a sitios web de verificación y/o listados de correo que suministren información sobre los códigos maliciosos nuevos;

h) implementación de procedimientos para verificar la información relacionada con códigos maliciosos y garantizar que los boletines de advertencia sean exactos e informativos; los directores deberían garantizar que se utilizan fuentes calificadas, por ejemplo diarios reconocidos, sitios confiables de Internet o proveedores de software de protección contra códigos maliciosos para diferenciar entre falsas alarmas y códigos maliciosos reales; todos los usuarios deberían conocer el problema de los falsas alarmas y qué hacer al recibirlas.

*Información adicional*
El empleo de dos o más productos de software, de diferentes proveedores, que protejan contra códigos maliciosos a través de todo el entorno de procesamiento de información puede mejorar la eficacia de la protección contra códigos maliciosos.

El software de protección contra códigos maliciosos se puede instalar para que suministre actualizaciones automáticas de los archivos de definición y de los motores de exploración para garantizar que la protección esté al día. Además, este software se puede instalar en cada escritorio para realizar verificaciones automáticas.

Se debe tener cuidado para la protección contra la introducción de códigos maliciosos durante los procedimientos de mantenimiento y de emergencia, ya que se pueden eludir los controles normales de protección contra códigos maliciosos.

### *10.4.2 Controles contra códigos móviles*

*Control*
Cuando se autoriza la utilización de códigos móviles, la configuración debería asegurar que dichos códigos operan de acuerdo con la política de la seguridad claramente definida, y se debería evitar la ejecución de los códigos móviles no autorizados.

*(Continúa)*

*Guía de implementación*
Se recomienda tener en cuenta las siguientes consideraciones para la protección contra códigos móviles que ejecutan acciones no autorizadas:

a) ejecución de los códigos móviles en un entorno con aislamiento lógico;

b) bloqueo de cualquier uso de códigos móviles;

c) bloqueo de la recepción de códigos móviles;

d) activación de medidas técnicas, según estén disponibles, en un sistema específico para garantizar la gestión del código móvil;

e) control de recursos disponibles para el acceso a códigos móviles;

f) controles criptográficos para autenticar de forma única el código móvil.

*Información adicional*
El código móvil es un código de software que se transfiere de un computador a otro y luego se ejecuta automáticamente y lleva a cabo una función específica con poca o ninguna interacción del usuario. El código móvil se asocia con una variedad de servicios intermedios (*middleware*).

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

## 10.5 Respaldo

Objetivo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Se deberían establecer procedimientos de rutina para implementar la política y la estrategia de respaldo acordada (véase el numeral 14.1) para hacer copias de la seguridad de los datos y probar sus tiempos de restauración.

### *10.5.1 Respaldo de la información*

*Control*
Se deberían hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.

*Guía de implementación*
Es conveniente disponer de servicios de respaldo adecuados para garantizar que la información y el software esenciales se recuperan después de un desastre o una falla de los medios.

Se recomienda considerar los siguientes elementos para el respaldo de la información:

a) es recomendable definir el nivel necesario para la información de respaldo;

b) se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos documentados de restauración;

c) la extensión (por ejemplo respaldo completo o diferencial) y la frecuencia de los respaldos debería reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada y la importancia de la operación continúa de la organización;

d) los respaldos se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres en la sede principal;

e) a la información de respaldo se le debería dar un grado apropiado de protección física y ambiental (véase el numeral 9) consistente con las normas aplicadas en la sede principal; los controles aplicados a los medios en la sede principal se deberían extender para cubrir el sitio en donde está el respaldo;

*(Continúa)*

f) es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario;

g) los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficacia y que se pueden completar dentro del tiempo designado en los procedimientos operativos para la recuperación;

h) en situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Las disposiciones de respaldo para los sistemas individuales se deberían someter a prueba con regularidad para garantizar que cumplen los requisitos de los planes para la continuidad del negocio (véase la sección 14). Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

Es necesario determinar el periodo de retención de la información esencial para el negocio, así como cualquier requisito para retener permanentemente las copias de archivo (véase el numeral 15.1.3).

*Información adicional*
Las disposiciones de respaldo se pueden automatizar para facilitar el respaldo y el proceso de restauración. Las soluciones automatizadas deberían probarse suficientemente antes de la implementación y a intervalos regulares.

## 10.6 Gestión de la seguridad de las redes

Objetivo: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

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

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

### *10.6.1 Controles de las redes*

*Control*
Las redes se deberían mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.

*Guía de implementación*
Los directores de la red deberían implementar controles que garanticen la seguridad de la información sobre las redes y la protección de los servicios conectados contra el acceso no autorizado. En particular, es conveniente tener en cuenta los siguientes elementos:

a) la responsabilidad operativa por las redes debería estar separada de las operaciones de computador, según sea apropiado (véase el numeral 10.1.3);

b) es necesario establecer las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios;

c) es conveniente establecer controles especiales para salvaguardar la confidencialidad y la integridad de los datos que pasan por redes públicas o redes inalámbricas y para proteger los sistemas y las aplicaciones conectadas (véanse los numerales 11.4 y 12.3); también se pueden requerir controles especiales para mantener la disponibilidad de los servicios de la red y los computadores conectados;

*(Continúa)*

d) se deberían aplicar el registro y el monitoreo adecuados para permitir el registro de acciones de la seguridad pertinentes;

e) se recomienda coordinar estrechamente las actividades de gestión tanto para optimizar el servicio para la organización como para garantizar que los controles se aplican consistentemente en toda la infraestructura del procesamiento de información.

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

***10.6.2 Seguridad de los servicios de la red***

*Control*
En cualquier acuerdo sobre los servicios de la red se deberían identificar e incluir las características de la seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de la red, sin importar si los servicios se prestan en la organización o se contratan externamente.

*Guía de implementación*
La capacidad del proveedor del servicio de red para gestionar los servicios acordados de forma segura se debería determinar y monitorear regularmente, y se debería acordar el derecho a auditoría.

Se deberían identificar las disposiciones de la seguridad necesarias para servicios particulares, tales como las características de la seguridad, los niveles de servicio y los requisitos de gestión.

La organización debería garantizar que los proveedores de servicios de red implementan estas medidas.

*Información adicional*
Los servicios de red incluyen la provisión de conexiones, servicios de red privada y redes con valor agregado, así como soluciones de la seguridad de red administrada, como por ejemplo cortafuegos (*Firewalls*) y sistemas de detección de intrusión. Estos servicios pueden ir desde simples anchos de banda no administrados hasta ofertas complejas de valor agregado.

Las características de los servicios de red podrían ser:

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

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

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

## 10.7 Manejo de los medios

Objetivos: evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio.

Estos medios se deberían controlar y proteger de forma física.

Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada/salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

*(Continúa)*

***10.7.1 Gestión de los medios removibles***

*Control*
Se deberían establecer procedimientos para la gestión de los medios removibles.

*Guía de implementación*
Se recomienda tener presentes las siguientes directrices:

a) si ya no son necesarios, los contenidos de todos los medios reutilizables que se van a retirar de la organización se deberían hacer irrecuperables;

b) cuando sea necesario y práctico, se debería exigir autorización para los medios retirados de la organización y conservar un registro de tales retiros para mantener una prueba de auditoría;

c) todos los medios se deberían almacenar en un ambiente seguro y vigilado, según las especificaciones del fabricante;

d) la información almacenada en los medios que debe estar disponible por más tiempo del de la vida del medio (según las especificaciones del fabricante) también se debería almacenar en otra parte para evitar la pérdida de información debido al deterioro de dichos medios;

e) se debería tener en cuenta el registro de los medios removibles para evitar la oportunidad de que se presente pérdida de datos;

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

Todos los procedimientos y niveles de autorización deberían estar documentados con claridad.

*Información adicional*
Los medios removibles incluyen cintas, discos, memorias de almacenamiento, unidades de almacenamiento removibles, discos compactos, discos de video digital (DVD) y medios impresos.

***10.7.2 Eliminación de los medios***

*Control*
Cuando ya no se requieren estos medios, su eliminación se debería hacer de forma segura y sin riesgo, utilizando los procedimientos formales.

*Guía de implementación*
Los procedimientos formales para la eliminación segura de los medios deberían minimizar el riesgo de fuga de información sensible a personas no autorizadas. Los procedimientos para la eliminación segura de los medios que contienen información sensible deberían estar acordes con la sensibilidad de dicha información. Se recomienda tener en cuenta los siguientes elementos.

a) los medios que contienen información sensible se deberían almacenar y eliminar de forma segura e inocua, por ejemplo mediante incineración o trituración, o borrar los datos para evitar el uso por parte de otra aplicación en la organización;

b) se deberían establecer procedimientos para identificar los elementos que pueden requerir eliminación segura;

c) puede ser más fácil disponer de todos los elementos de los medios de almacenamiento que serán recogidos y liberados de forma segura, que tratar de disponer sólo de los elementos sensibles;

d) muchas organizaciones ofrecen servicios de recolección y eliminación de papel, equipos y medios; se debe tener cuidado en seleccionar un contratista idóneo con controles y experiencia adecuados;

e) cuando sea posible, se debería registrar la eliminación de los elementos sensibles con el objeto de mantener una prueba de auditoría.

*(Continúa)*

Cuando se acumulan medios para su eliminación se debería considerar el efecto de agregación, el cual puede hacer que una gran cantidad de información no sensible se vuelva sensible.

*Información adicional*
Se podría divulgar información sensible debido a la eliminación descuidada del medio (véase el numeral 9.2.6 para información sobre la eliminación del equipo).

***10.7.3 Procedimientos para el manejo de la información***

*Control*
Se deberían establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.

*Guía de implementación*
Se deberían elaborar procedimientos para manejar, procesar, almacenar y comunicar la información de acuerdo con su clasificación (véase el numeral 7.2). Se deberían considerar los siguientes elementos:

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

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

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

d) garantizar que los datos de entrada están completos, que el procesamiento se completa adecuadamente y que se aplica la validación de la salida;

e) protección, según su nivel de sensibilidad, de los datos de la memoria temporal que esperan su ejecución;

f) almacenamiento de los medios según las especificaciones del fabricante;

g) mantenimiento de la distribución de datos en un mínimo;

h) rotulado claro de todas las copias de los medios para la autenticación del receptor autorizado;

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

*Información adicional*
Estos procedimientos se aplican a la información en documentos, sistemas de computación, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, prestaciones / servicios postales, uso de máquinas de fax y a todos los elementos sensibles, como cheques en blanco y facturas.

***10.7.4 Seguridad de la documentación del sistema***

*Control*
La documentación del sistema debería estar protegida contra el acceso no autorizado.

*Guía de implementación*
Para asegurar la documentación del sistema, se deberían tener en cuenta los siguientes elementos:

a) la documentación del sistema se debería almacenar con seguridad;

b) la lista de acceso a la documentación del sistema se debería mantener mínima y debería estar autorizada por el responsable de la aplicación;

c) la documentación del sistema en la red pública o que se suministra a través de una red pública, debería tener protección adecuada.

*(Continúa)*

*Información adicional*
La documentación del sistema puede contener variada información sensible, como descripciones de procesos de aplicación, procedimientos, estructuras de datos y procesos de autorización.

## 10.8 Intercambio de la información

Objetivo: mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.

Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, ejecutar según los acuerdos de intercambio y cumplir la legislación correspondiente (véase la sección 15).

Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito

### *10.8.1 Políticas y procedimientos para el intercambio de información*

*Control*
Se deberían establecer políticas, procedimientos y controles formales de intercambio para proteger la información mediante el uso de todo tipo de servicios de comunicación.

*Guía de implementación*
Los procedimientos y controles a seguir cuando se utilizan servicios de comunicación electrónica para el intercambio de información deberían considerar los siguientes elementos:

a) procedimientos diseñados para proteger la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción;

b) procedimientos para detección y protección contra códigos maliciosos que se pueden transmitir con el uso de comunicaciones electrónicas (véase el numeral 10.4.1);

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

d) políticas o directrices que enfaticen el uso aceptable de los servicios de comunicación electrónica (véase el numeral 7.1.3);

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

f) responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer a la organización, por ejemplo a través de difamación, acoso, suplantación de identidad, envío de cartas de cadena, adquisición no autorizada, etc.;

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

h) directrices de retención y eliminación para toda la correspondencia, incluyendo mensajes, según la legislación y los reglamentos locales y nacionales correspondientes;

i) no dejar información sensible o crítica en los dispositivos de impresión como copiadoras, impresoras y máquinas de fax ya que se puede permitir el acceso de personal no autorizado;

j) controles y restricciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas;

k) recordar al personal que deberían tomar precauciones adecuadas como, por ejemplo, no revelar información sensible para evitar que, cuando se hace una llamada telefónica, sea interceptada o escuchada por:

*(Continúa)*

1) personas en la cercanía inmediata, particularmente cuando se utilizan teléfonos móviles;

2) intercepciones telefónicas u otras formas de escuchas no autorizadas mediante el acceso físico al auricular o a la línea telefónica, o usando receptores de exploración;

3) personal al lado del receptor;

l) no dejar mensajes que contengan información sensible en el contestador automático ya que pueden volver a ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación errónea;

m) recordar al personal sobre los problemas de usar máquinas de fax, principalmente:

1) creación de acceso no autorizado en los almacenes de mensajes para recuperar los mensajes;

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

3) envío de documentos y mensajes al número equivocado, bien sea por marcación errónea o por usar el número almacenado erróneamente;

n) recordar al personal no registrar datos demográficos, como direcciones de correo electrónico u otra información personal, en ningún software para evitar su recolección para uso no autorizado;

o) recordar al personal que las máquinas modernas de fax y las fotocopiadoras tienen páginas de almacenamiento y cache, en caso de falla en el papel o en la transmisión, que se pueden imprimir una vez se ha solucionado la falla.

Además, se debería recordar al personal que no debería tener conversaciones confidenciales en lugares públicos ni oficinas abiertas, como tampoco en lugares de reunión sin paredes a prueba de sonido:

Los servicios de intercambio de información deberían cumplir todos los requisitos legales pertinentes (véase el numeral 15).

*Información adicional*
El intercambio de información se puede producir a través de la utilización de diferentes tipos de servicios de comunicación, incluyendo correo electrónico, voz, fax y video.

El intercambio de software se puede dar a través de diferentes medios, incluyendo descargas desde Internet y adquiridas de vendedores de productos de mostrador.

El negocio debería considerar las implicaciones legales y de la seguridad asociadas con el intercambio electrónico de datos, el comercio electrónico y las comunicaciones electrónicas, así como los requisitos para los controles.

La información podría verse amenazada debido a la falta de conciencia, de políticas o procedimientos sobre el uso de los servicios de intercambio de información, por ejemplo por la escucha en un teléfono móvil en un lugar público, la dirección incorrecta de un mensaje de correo electrónico, la escucha de los contestadores automáticos, el acceso no autorizado a sistemas de correo de voz de marcación o el envío accidental de facsímiles al equipo errado de fax.

Las operaciones del negocio podrían ser afectadas y la información podría ser comprometida si los servicios de comunicación fallan, se sobrecargan o interrumpen (véase el numeral10.3 y el numeral 14). La información se vería comprometida por el acceso de usuarios no autorizados (véase el numeral 11).

***10.8.2 Acuerdos para el intercambio***

*Control*
Se deberían establecer acuerdos para el intercambio de la información y del software entre la organización y las partes externas.

*(Continúa)*

*Guía de implementación*
En los acuerdos de intercambio se deberían tomar en consideración las siguientes condiciones de la seguridad:

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

b) procedimientos para notificar a quien envía la transmisión, el despacho y la recepción;

c) procedimientos para garantizar la trazabilidad y el no-repudio;

d) normas técnicas mínimas para el empaquetado y la transmisión;

e) acuerdos de fideicomiso;

f) normas para identificar los servicios de mensajería;

g) responsabilidades y deberes en caso de incidentes de la seguridad de la información, como la pérdida de datos;

h) uso de sistemas acordados de etiquetado de la información sensible o crítica, garantizando que el significado de las etiquetas se entienda inmediatamente y que la información está protegida adecuadamente;

i) propiedad y responsabilidades para la protección de datos, derechos de copia, conformidad de las licencias de software y consideraciones similares (véanse los numerales 15.1.2 y 15.1.4);

j) normas técnicas para registrar y leer la información y el software;

k) todos los controles especiales que se puedan requerir para proteger los elementos sensibles tales como las claves criptográficas (véase el numeral 12.3).

Se deberían establecer y conservar políticas, procedimientos y normas para proteger la información y los medios físicos en tránsito (véase el numeral 10.8.3) y ellos se deberían referenciar en dichos acuerdos de intercambio.

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

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

***10.8.3 Medios físicos en tránsito***

*Control*
Los medios que contienen información se deberían proteger contra el acceso no autorizado, el uso inadecuado o la corrupción durante el transporte más allá de los límites físicos de la organización.

*Guía de implementación*
Se recomienda tener en cuenta las siguientes directrices para la protección de los medios que se transportan entre los lugares:

a) se recomienda utilizar transporte confiable o servicios de mensajería;

b) se debería acordar con la dirección una lista de servicios de mensajería;

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

*(Continúa)*

d) el embalaje debería ser suficiente para proteger el contenido contra cualquier daño físico potencial que se pueda producir durante el transporte, y estar acorde con las especificaciones del fabricante (por ejemplo para el software), por ejemplo protección contra todos los factores ambientales que puedan reducir la eficacia de la restauración de los medios tal como la exposición al calor, la humedad o los campos electromagnéticos;

e) Cuando sea necesario, se deberían adoptar controles para proteger la información sensible contra divulgación o modificación no autorizada; algunos ejemplos incluyen;

1) uso de contenedores cerrados con llave;

2) entrega personal;

3) embalajes con sello de la seguridad (que revelan cualquier intento de acceso);

4) en casos excepcionales, división de la remesa en más de una entrega y despacho por rutas diferentes.

*Información adicional*
La información puede ser vulnerable al acceso no autorizado, al uso inadecuado o a la corrupción durante el transporte físico, es el caso de los envíos de medios a través de servicios postales o de mensajería.

### *10.8.4 Mensajería electrónica*

*Control*
La información contenida en la mensajería electrónica debería tener la protección adecuada.

*Guía de implementación*
Las consideraciones de la seguridad para la mensajería electrónica deberían incluir las siguientes:

a) proteger los mensajes contra acceso no autorizado, modificación o negación de los servicios;

b) garantizar que la dirección y el transporte del mensaje son correctos;

c) confiabilidad general y disponibilidad del servicio;

d) consideraciones legales como, por ejemplo, los requisitos para las firmas electrónicas;

e) obtención de aprobación antes de utilizar servicios públicos externos como la mensajería instantánea o el compartir archivos;

f) niveles más sólidos de autenticación que controlen el acceso desde redes accesibles al público.

*Información adicional*
La mensajería electrónica como, por ejemplo, el correo electrónico, el intercambio de datos electrónicos (EDI) y la mensajería instantánea tienen una función cada vez más creciente en las comunicaciones de los negocios. La mensajería electrónica tiene riesgos diferentes que las comunicaciones en papel.

### *10.8.5 Sistemas de información del negocio*

*Control*
Se deberían establecer, desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

*Guía de implementación*
Las consideraciones de las implicaciones que tiene la interconexión de tales servicios para la seguridad y para el negocio deberían incluir:

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

*(Continúa)*

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

c) política y controles adecuados para gestionar la forma en que se comparte la información;

d) categorías excluyentes de información sensible para la organización y documentos clasificados, si los sistemas no brindan un nivel adecuado de protección;

e) restricción del acceso a la información diaria relacionada con individuos seleccionados, por ejemplo el personal que trabaja en proyectos sensibles;

f) categorías de personal, contratistas o socios del negocio a quienes se permite usar el sistema y los sitios desde los cuales pueden tener acceso;

g) restricción de los servicios seleccionados para categorías de usuarios específicos;

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

i) retención y copias de respaldo de la información contenida en el sistema (véase el numeral 10.5.1);

j) requisitos y disposiciones para los recursos de emergencia (véase el numeral 14).

*Información adicional*
Los sistemas de información de las oficinas son oportunidades para diseminar y compartir más rápido la información del negocio utilizando una combinación de: documentos, computadores, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios / prestaciones postales y máquinas de fax.

## 10.9 Servicios de comercio electrónico

Objetivo: garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.

Es necesario considerar las implicaciones de la seguridad asociadas al uso de servicios de comercio electrónico, incluyendo las transacciones en línea y los requisitos para los controles.

También se deberían considerar la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

### *10.9.1 Comercio electrónico*

*Control*
La información involucrada en el comercio electrónico que se transmite por las redes públicas debería estar protegida contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizada.

*Guía de implementación*
Las consideraciones de la seguridad para el comercio electrónico deberían incluir las siguientes:

a) el nivel de confianza que exige cada parte en la identidad declarada de las otras partes, por ejemplo por medio de autenticación;

b) los procesos de autorización asociados con la persona que puede establecer precios, emitir o firmar documentos comerciales clave;

c) la garantía de que los socios comerciales están totalmente informados sobre sus autorizaciones;

*(Continúa)*

d) la determinación y el cumplimiento de los requisitos de confidencialidad, integridad, prueba de despacho y recibo de documentos clave, y el no repudio de contratos, por ejemplo los asociados a los procesos de licitación y contratos;

e) el nivel de confianza exigido en la integridad de las listas publicadas de precios;

f) la confidencialidad de datos o información sensible;

g) la confidencialidad e integridad de las transacciones de orden de compra, información sobre pagos, detalles de las direcciones de entrega y confirmación de recibo;

h) el grado adecuado de verificación para comprobar la información sobre pagos suministrada por un cliente;

i) la selección del mejor convenio sobre la forma de pago más apropiada para evitar el fraude;

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

k) la evitación de la pérdida o duplicación de la información sobre transacciones;

l) la responsabilidad asociada con transacciones fraudulentas;

m) los requisitos de las pólizas de seguros.

Muchas de las consideraciones anteriores se pueden abordar mediante la aplicación de controles criptográficos (véase el numeral 12.3), teniendo en cuenta el cumplimiento de los requisitos legales (véase el numeral 15.1, especialmente el numeral 15.1.6 para la legislación criptográfica).

Los acuerdos de comercio electrónico entre socios comerciales deberían estar sustentados por un acuerdo documentado que comprometa a ambas partes con los términos acordados, incluyendo detalles sobre la autorización (véase b) arriba). Pueden ser necesarios otros acuerdos con los proveedores del servicio de información y de la red con valor agregado.

Los sistemas de comercio público deberían publicar sus términos del negocio a los clientes.

También se debería considerar la resistencia al ataque del servidor central (host) utilizado para el comercio electrónico y las implicaciones de la seguridad de cualquier interconexión de red necesaria para la implementación de los servicios de comercio electrónico (véase el numeral 11.4.6).

*Información adicional*
El comercio electrónico es vulnerable a una variedad de amenazas en la red que pueden ocasionar actividad fraudulenta, disputas por contratos y divulgación o modificación de información.

El comercio electrónico puede utilizar métodos de autenticación seguros, por ejemplo el uso de criptografía clave pública y firmas digitales (véase el numeral 12.3) para reducir el riesgo. También se pueden utilizar terceras partes confiables, cuando se necesitan tales servicios.

***10.9.2 Transacciones en línea***

*Control*
La información involucrada en las transacciones en línea debería estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

*Guía de implementación*

Las consideraciones de la seguridad para las transacciones en línea deberían incluir las siguientes:

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

*(Continúa)*

b) todos los aspectos de la transacción, es decir, garantizar que:

1) las credenciales de usuario de todas las partes son válidas y se han verificado;

2) la transacción sigue siendo confidencial; y

3) se conserva la privacidad asociada con todas las partes;

c) encriptación de la ruta para las comunicaciones entre todas las partes involucradas;

d) seguridad de los protocolos utilizados para la comunicación entre todas las partes involucradas;

e) garantizar que el almacenamiento de los detalles de la transacción está fuera de cualquier entorno de acceso público, por ejemplo en una plataforma de almacenamiento existente en la Intranet de la organización, y que no se retiene ni expone en un medio de almacenamiento accesible directamente desde Internet;

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

*Información adicional*
La extensión de los controles adoptados deberá estar acorde con el nivel de riesgo asociado con cada una de las formas de transacción en línea.

Puede ser necesario que las transacciones cumplan las leyes, las reglas y los reglamentos en la jurisdicción en la cual se genera la transacción, se procesa, se termina y/o almacena.

Existen muchas formas de transacciones que se pueden efectuar en línea, por ejemplo contractuales, financieras, etc.

***10.9.3 Información disponible al público***

*Control*
La integridad de la información que se pone a disposición en un sistema de acceso público debería estar protegida para evitar la modificación no autorizada.

*Guía de implementación*
El software, los datos y otra información que requiere un nivel alto de integridad que se pone a disposición en sistemas públicos se debería proteger con mecanismos apropiados como firmas digitales (véase el numeral 12.3). Los sistemas de acceso público se deberían probar frente a debilidades y fallas antes de que la información esté disponible.

Debería existir un proceso formal de aprobación previo a que la información esté disponible al público. Además, todas las entradas suministradas desde el exterior del sistema se deberían verificar y aprobar.

Los sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y entrada directa de información, se deberían controlar cuidadosamente de modo que:

a) la información se obtenga de conformidad con toda la legislación sobre protección de datos (véase el numeral 15.1.4);

b) la entrada de información hacia y procesada por el sistema de publicación se procese completa y exactamente de forma oportuna;

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

d) el acceso al sistema de publicación no permite acceso involuntario a redes a las cuales se conecta el sistema.

*(Continúa)*

*Información adicional*
Puede ser necesario que la información en un sistema disponible al público, por ejemplo la información en un servidor web accesible a través de Internet, cumpla las leyes, las reglas y los reglamentos en la jurisdicción en la cual se localiza el sistema, donde tiene lugar el intercambio o donde reside el responsable. La modificación no autorizada de la información pública puede dañar la reputación de la organización de la publicación.

## 10.10 Monitoreo

Objetivo: detectar actividades de procesamiento de la información no autorizadas.

Se deberían monitorear los sistemas y registrar los eventos de la seguridad de la información. Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de información.

Una organización debería cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro.

Debería emplearse el monitoreo del sistema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

### *10.10.1 Registro de auditorías*

*Control*
Se deberían elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de la seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.

*Guía de implementación*
Los registros para auditoría deberían incluir, cuando corresponda.

a) identificación (ID) de usuario;

b) fecha, hora y detalles de los eventos clave, por ejemplo registro de inicio y registro de cierre;

c) identidad o ubicación del terminal, si es posible;

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

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

f) cambios en la configuración del sistema;

g) uso de privilegios;

h) uso de las utilidades y aplicaciones del sistema;

i) archivos a los que se ha tenido acceso y tipo de acceso;

j) direcciones y protocolos de red;

k) alarmas originadas por el sistema de control del acceso;

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

*Información adicional*
Los registros para auditoría pueden contener datos personales confidenciales e indiscretos. Se deberían tomar medidas adecuadas para la protección de la privacidad (véase el numeral 15.1.4). Cuando sea posible, los administradores del sistema no deberían tener autorización para borrar ni desactivar registros de sus propias actividades (véase el numeral 10.1.3).

*(Continúa)*

***10.10.2 Monitoreo de uso del sistema***

*Control*
Se deberían establecer procedimientos para el monitoreo de uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deberían revisar con regularidad.

*Guía de implementación*
El nivel de monitoreo necesario para servicios individuales se debería determinar mediante una evaluación de riesgos. La organización debería cumplir todos los requisitos legales que se apliquen a sus actividades de monitoreo. Las áreas que se deberían considerar incluyen:

a) acceso autorizado, incluyendo detalles como:

1) identificación de usuario (ID);

2) fecha y hora de eventos clave;

3) tipo de eventos;

4) archivos a los que se ha tenido acceso;

5) programas / utilidades empleados;

b) todas las operaciones privilegiadas como:

1) uso de cuentas privilegiadas, por ejemplo supervisor, raíz, administrador;

2) encendido y detención del sistema;

3) acople / desacople del dispositivo de entrada / salida (I/O);

c) intentos de acceso no autorizado, tales como:

1) acciones de usuario fallidas o rechazadas;

2) acciones fallidas o rechazadas que implican datos y otros recursos;

3) violaciones de la política de acceso y notificaciones para los cortafuegos (firewalls) y puertas de enlace (gateways);

4) alertas de los sistemas de detección de intrusión de responsable;

d) alertas o fallas del sistema como:

1) alertas o mensajes de consola;

2) excepciones de registro del sistema;

3) alarmas de gestión de red;

4) alarmas originadas por el sistema de control del acceso;

e) cambios o intentos de cambio en la configuración y los controles de la seguridad del sistema.

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

a) importancia de los procesos de aplicación;

b) valor, sensibilidad e importancia de la información implicada;

*(Continúa)*

c) experiencia previa de infiltración o uso inadecuado del sistema, y frecuencia de aprovechamiento de las vulnerabilidades;

d) extensión de la interconexión del sistema (particularmente en redes públicas);

e) registro del servicio de operación que se desactiva.

*Información adicional*
Es necesario el uso de procedimientos de monitoreo para garantizar que los usuarios únicamente ejecutan actividades autorizadas explícitamente.

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

***10.10.3 Protección del registro de la información***

*Control*
El registro del servicio y la información se deberían proteger contra el acceso o la manipulación no autorizados.

*Guía de implementación*
Los controles deberían tener como objeto la protección contra cambios no autorizados y problemas operativos con el registro del servicio incluyendo:

a) alteraciones en los tipos de mensaje que se registran;

b) archivos de registro que se editan o eliminan;

c) capacidad de almacenamiento que se excede del archivo del registro, lo que produce ya sea en la falla para grabar eventos o sobre-escritura de eventos grabados anteriormente.

Puede ser necesario archivar algunos registros para auditoría como parte de la política de retención de registros o debido a los requisitos para recolectar y conservar evidencia (véase el numeral 13.2.3).

*Información adicional*
Los registros del sistema a menudo contienen un gran volumen de información, mucha de la cual no tiene relación con el monitoreo de la seguridad. Para facilitar la identificación de los eventos significativos para propósitos del monitoreo de la seguridad, se debería considerar el copiado automático de los tipos apropiados de mensaje en un segundo registro y / o el uso de utilidades del sistema adecuadas o de herramientas de auditoría para realizar la interrogación y racionalización del archivo.

Es necesario proteger los registros del sistema porque si sus datos se pueden modificar o eliminar, su existencia puede crear un sentido falso de la seguridad.

***10.10.4 Registros del administrador y del operador***

*Control*
Se deberían registrar las actividades tanto del operador como del administrador del sistema.

*Guía de implementación*
Los registros deberían incluir:

a) la hora en que ocurrió el evento (exitoso o fallido);

b) información sobre el evento (por ejemplo archivos manipulados) o la falla (por ejemplo errores que se presentaron y acciones correctivas que se tomaron);

c) cuál cuenta y cuál administrador u operador estuvo involucrado;

*(Continúa)*

d) cuáles procesos estuvieron implicados.

Los registros del operador y del administrador del sistema se deberían revisar con regularidad.

*Información adicional*
Se puede emplear un sistema de detección de intrusos que esté fuera del control del sistema y de los administradores de red para monitorear el cumplimiento de las actividades del sistema y de la administración de la red.

***10.10.5 Registro de fallas***

*Control*
Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas.

*Guía de implementación*
Se deberían registrar las fallas reportadas por los usuarios o por los programas del sistema relacionadas con problemas de procesamiento de la información o con los sistemas de comunicación. Deberían existir reglas claras para el manejo de las fallas reportadas, incluyendo:

a) revisión de los registros de fallas para garantizar que éstas se han resuelto satisfactoriamente;

b) revisión de las medidas correctivas para garantizar que no se han puesto en peligro los controles y que la acción tomada está totalmente autorizada.

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

*Información adicional*
El registro de errores y de fallas puede tener impacto en el desempeño del sistema. Dicho registro debería ser habilitado por personal competente y el nivel necesario de registro para sistemas individuales se debería determinar mediante una evaluación de riesgos, teniendo en cuenta el deterioro del desempeño.

***10.10.6 Sincronización de relojes***

*Control*
Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de la seguridad deberían estar sincronizados con una fuente de tiempo exacta y acordada.

*Guía de implementación*
Cuando un computador o un dispositivo de comunicaciones tiene la capacidad para operar un reloj en tiempo real, dicho reloj se debería establecer como el estándar acordado, por ejemplo el tiempo coordinado universal (UTC) o el tiempo estándar local.

Debido a que se sabe que algunos relojes varían con el paso del tiempo, debería existir un procedimiento que verifique y corrija cualquier variación significativa.

La interpretación correcta del formato fecha/hora es importante para garantizar que la marca de tiempo refleja la fecha/hora real. Es conveniente tener en cuenta las especificaciones locales (por ejemplo el horario de verano).

*Información adicional*
La configuración correcta de los relojes del computador es importante para garantizar la exactitud de los registros para auditoría, lo cual puede ser necesario para las investigaciones o como evidencia en casos disciplinarios o legales. Los registros inexactos de auditoría pueden dificultar dichas investigaciones y deteriorar la credibilidad de la evidencia. Se puede utilizar un reloj sincronizado a un reloj atómico nacional el cual es tomado como reloj maestro para los sistemas de acceso. También se puede usar un protocolo de tiempo de red para mantener todos los servidores en sincronización con el reloj maestro.

*(Continúa)*

# 11. Control del acceso

## 11.1 Requisitos del negocio para el control del acceso

Objetivo: controlar el acceso a la información.

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de la seguridad y del negocio.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

### *11.1.1 Política de control de acceso*

*Control*
Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

*Guía de implementación*
Las reglas y los derechos para el control del acceso para cada usuario o grupo de usuarios se deberían establecer con claridad en una política de control del acceso. Los controles del acceso son tanto lógicos como físicos (véase la sección 9) y se deberían considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) requisitos de la seguridad de las aplicaciones individuales del negocio;

b) identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información;

c) políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de la seguridad y la clasificación de la información (véase el numeral 7.2);

d) consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes;

e) legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios (véase el numeral 15.1);

f) perfiles estándar de acceso de usuario para funciones laborales comunes en la organización;

g) gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles;

h) distribución de las funciones de control de acceso, por ejemplo solicitud de acceso, autorización del acceso, administración del acceso;

i) requisitos para la autorización formal de las solicitudes de acceso (véase el numeral 11.2.1);

j) requisitos para la revisión periódica de los controles de acceso (véase el numeral 11.2.4);

k) retiro de los derechos de acceso (véase el numeral 8.3.3).

*Información adicional*
Se recomienda cuidado al especificar las reglas de control de acceso para considerar:

a) diferenciación entre reglas que siempre se deben hacer cumplir y directrices que son opcionales o condicionales;

*(Continúa)*

b) establecimiento de reglas basadas en la premisa "En general, todo está prohibido, a menos que esté expresamente permitido" y no en la regla más débil de " En general, todo está permitido, a menos que esté expresamente prohibido";

c) cambios en las etiquetas de la información (véase el numeral 7.2) que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados a discreción del usuario;

d) cambios en los permisos de usuario que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados por un administrador;

e) reglas que requieren aprobación específica antes de su promulgación y aquellas que no.

Las reglas de control de acceso deberían tener soporte de procedimientos formales y de responsabilidades claramente definidas (véase, por ejemplo, 6.1.3, 11.3, 10.4.1, 11.6).

## 11.2 Gestión del acceso de usuarios

Objetivo: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.
Los procedimientos deberían comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información.

Se debería poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

### *11.2.1 Registro de usuarios*

*Control*
Debería existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

*Guía de implementación*
El procedimiento de control del acceso para el registro y cancelación de usuarios debería incluir:

a) uso de la identificación única de usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o del negocio, y deberían estar aprobados y documentados;

b) verificación de que el usuario tenga autorización del responsable del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección apruebe por separado los derechos de acceso;

c) verificación de que el nivel de acceso otorgado sea adecuado para los propósitos del negocio (véase el numeral 11.1) y sea consistente con la política de la seguridad de la organización, es decir, no pone en peligro la distribución de funciones (véase el numeral 10.1.3);

d) dar a los usuarios una declaración escrita de sus derechos de acceso;

e) exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso;

*(Continúa)*

f) asegurar que los proveedores del servicio no otorguen el acceso hasta que se hallan terminado los procedimientos de autorización;

g) mantenimiento de un registro formal de todas las personas registradas para usar el servicio;

h) retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización;

i) verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios (véase el numeral 11.2.4);

j) garantizar que las identificaciones (ID) de usuario redundantes no se otorgan a otros usuarios.

*Información adicional*
Se debería considerar el establecimiento de roles de acceso de usuario basadas en los requisitos del negocio que incluyan un número de derechos en perfiles típicos de acceso de usuario. Las solicitudes y revisiones de acceso (véase el numeral 11.2.4) se gestionan más fácilmente en el ámbito de dichas funciones que en el ámbito de derechos particulares.

Es conveniente considerar la inclusión de cláusulas en los contratos del personal y de los servicios que especifiquen las sanciones si el personal o los agentes del servicio intentan el acceso no autorizado (véanse los numerales 6.1.5, 8.1.3 y 8.2.3).

***11.2.2 Gestión de privilegios***

*Control*
Se debería restringir y controlar la asignación y el uso de privilegios.

*Guía de implementación*
Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían controlar la asignación de privilegios a través de un proceso formal de autorización.

Se recomienda tener en cuenta los siguientes elementos:

a) Se deberían identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de bases de datos y aplicaciones;

b) Se deberían asignar los privilegios a los usuarios sobre los principios de necesidad-de uso y evento-por-evento, y de manera acorde con la política de control de acceso (véase el numeral 11.1.1), es decir, el requisito mínimo para su función, sólo cuando sea necesario;

c) se deberían conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se deberían otorgar hasta que el proceso de autorización esté completo;

d) es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios;

e) se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios;

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

*Información adicional*
El uso no apropiado de los privilegios de administración del sistema (cualquier característica o servicio de un sistema que permita al usuario anular los controles del sistema o de la aplicación) puede ser un factor contribuyente importante a las fallas o vulnerabilidades del sistema.

***11.2.3 Gestión de contraseñas para usuarios***

*Control*
La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

*(Continúa)*

*Guía de implementación*
El proceso debería incluir los siguientes requisitos:

a) se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales (véase el numeral 8.1.3);

b) cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura (véase el numeral 11.3.1) que estén forzados a cambiar inmediatamente;

c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva;

d) las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro);

e) las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables;

f) los usuarios deberían confirmar la entrega de las contraseñas;

g) las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido;

h) las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.

*Información adicional*
Las contraseñas son un medio común de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información de acuerdo con la autorización del usuario.

Según el caso, es recomendable considerar otras tecnologías disponibles para la identificación y autenticación del usuario tales como biométricos, (verificación de huella digital, verificación de firma) y el uso de *tokens* de autenticación, (tarjetas inteligentes).

***11.2.4 Revisión de los derechos de acceso de los usuarios***

*Control*

La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

*Guía de implementación*

Se recomienda que en la revisión de los derechos de acceso se consideren las siguientes directrices:

a) los derechos de acceso de los usuarios se deberían revisar a intervalos regulares, por ejemplo cada seis meses y después de cada cambio, como por ejemplo promoción, cambio a un cargo en un nivel inferior, o terminación del contrato laboral (véase el numeral 11.2.1);

b) los derechos de acceso de usuarios se debería revisar y reasignar cuando hay cambios de un cargo a otro dentro de la misma organización;

c) es recomendable revisar las autorizaciones para derechos de acceso privilegiado (véase el numeral 11.2.2) a intervalos más frecuentes, por ejemplo cada tres meses;

d) se debería verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados;

e) los cambios en las cuentas privilegiadas se deberían registrar para su revisión periódica.

*(Continúa)*

*Información adicional*
Es necesario revisar con regularidad los derechos de acceso de los usuarios para mantener un control eficaz del acceso a los datos y a los servicios de información.

## 11.3 Responsabilidades de los usuarios

Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se debería concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.

### *11.3.1 Uso de contraseñas*

*Control*
Se debería exigir a los usuarios el cumplimiento de buenas prácticas de la seguridad en la selección y el uso de las contraseñas.

*Guía de implementación*
Todos los usuarios deberían:

a) mantener la confidencialidad de las contraseñas;

b) evitar conservar registros (por ejemplo en papel, archivos de software o dispositivos manuales) de las contraseñas, a menos que éstas se puedan almacenar de forma segura y el método de almacenamiento esté aprobado;

c) cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña;

d) seleccionar contraseñas de calidad con longitud mínima suficiente que:

   1) sean fáciles de recordar;

   2) no se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.;

   3) no sean vulnerables al ataque de diccionarios (es decir, que no consistan en palabras incluidas en diccionarios);

   4) no tengan caracteres idénticos consecutivos, que no sean todos numéricos ni todos alfabéticos;

e) cambiar las contraseñas a intervalos regulares o con base en el número de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas;

f) cambiar las contraseñas temporales en el primer registro de inicio;

g) no incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función;

h) no compartir las contraseñas de usuario individuales;

*(Continúa)*

i) no utilizar la misma contraseña para propósitos del negocio y para los que no lo son.

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que pueden usar una sola contraseña de calidad (véase d) arriba) para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable de protección para almacenar la contraseña en cada servicio, sistema o plataforma.

*Información adicional*
La gestión de los sistemas de ayuda del escritorio auxiliar que tratan con las contraseñas perdidas u olvidadas necesita cuidado especial puesto que también puede ser un medio de ataque al sistema de contraseña.

***11.3.2 Equipo de usuario desatendido***

*Control*
Los usuarios deberían asegurarse de que los equipos desatendidos tengan protección apropiada.

*Guía de implementación*
Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de la seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña;

b) realizar el registro de cierre en computadoras principales, servidores y computadores personales de oficina al terminar la sesión (es decir, no sólo apagar el interruptor de la pantalla del computador o terminal);

c) cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña (véase el numeral 11.3.3).

*Información adicional*
Los equipos instalados en las áreas de usuario, por ejemplo las estaciones de trabajo o los servidores de archivo, pueden requerir protección específica contra el acceso no autorizado cuando se dejen desatendidos durante periodos prolongados.

***11.3.3 Política de escritorio despejado y de pantalla despejada***

*Control*
Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

*Guía de implementación*
En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información (véase el numeral 7.2), los requisitos legales y contractuales (véase el numeral 15.1), los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) cuando no se requiere la información sensible o crítica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave (idealmente una caja fuerte, un gabinete u otro mueble de la seguridad), especialmente cuando la oficina está vacía;

b) las sesiones de los computadores y los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un *token* o un mecanismo similar de autenticación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando;

c) se deberían proteger los puntos de entrada y salida de correo y las máquinas de facsímil desatendidas;

*(Continúa)*

d) es conveniente evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, etc.).

e) los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.

*Información adicional*
Una política sobre escritorio despejado / pantalla despejada reduce los riesgos de acceso no autorizado, pérdida y daño de la información durante y fuera de las horas laborales normales.

Las cajas fuertes u otras formas de almacenamiento seguro también podrían proteger la información almacenada allí contra desastres como incendio, terremoto, inundación o explosión.

Se debería pensar en la utilización de impresoras con función de código de pines (*pin code*) de forma que quien inicia la impresión sea el único que pueda obtenerla y únicamente cuando esté cerca de la impresora.

## 11.4 Control de acceso a las redes

Objetivo: evitar el acceso no autorizado a los servicios en red.

Es recomendable controlar el acceso a los servicios en red, tanto internos como externos.

El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

a) existen interfases apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones, y las redes públicas;

b) se aplican mecanismos adecuados de autenticación para los usuarios y los equipos;

c) se exige control de acceso de los usuarios a los servicios de información.

### *11.4.1 Política de uso de los servicios en red*

*Control*
Los usuarios sólo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.

*Guía de implementación*
Se debería formular una política con respecto al uso de las redes y los servicios de red. Esta política debería abarcar:

a) las redes y los servicios de red a los cuales se permite el acceso;

b) los procedimientos de autorización para determinar a quién se le permite el acceso a qué redes y qué servicios en red;

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

d) los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de Internet o a un sistema remoto).

La política sobre el uso de los servicios de red debería ser consistente con la política de control de acceso de la organización (véase el numeral 11.1).

*(Continúa)*

*Información adicional*
Las conexiones inseguras y no autorizadas a servicios de red pueden afectar a toda la organización. Este control es particularmente importante para las conexiones de red de aplicaciones sensibles o críticas para el negocio o para usuarios en lugares de alto riesgo, por ejemplo en áreas públicas o externas que se hallan fuera del control y la gestión de la seguridad de la organización.

***11.4.2 Autenticación de usuarios para conexiones externas***

*Control*
Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

*Guía de implementación*
La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica con base criptográfica, *token* de hardware o protocolos de desafío / respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones de red privada virtual (VPN). Las líneas privadas dedicadas también se pueden emplear para brindar aseguramiento de la fuente de las conexiones.

Los procedimientos y controles de devolución de marcación, por ejemplo empleando módems de retorno de marcación, pueden suministrar protección contra conexiones no deseadas o no autorizadas a los servicios de procesamiento de información de la organización. Este tipo de control autentica a los usuarios tratando de establecer una conexión con una red de la organización desde sitios remotos. Cuando se usa este control, la organización no debería utilizar servicios de red que incluyen envío de llamada o, si lo hacen, deberían desactivar el uso de dichas características para evitar las debilidades asociadas con el envío de llamada. El proceso de devolución de llamada debería garantizar que realmente se produce una desconexión en el lado de la organización. De otro modo, el usuario remoto debería mantener la línea abierta pretendiendo que ha ocurrido la verificación de la devolución de la llamada. Los procedimientos y controles de devolución de la llamada se deberían probar en su totalidad para determinar esta posibilidad.

La autenticación del nodo puede servir como un medio alterno para la autenticación de grupos de usuarios remotos cuando están conectados a un servicio seguro de computador compartido. Para la autenticación del nodo se pueden emplear las técnicas criptográficas, por ejemplo las basadas en certificados de máquina. Esto forma parte de varias soluciones basadas en la red privada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas. En particular, es necesario tener cuidado especial en la selección de los controles para redes inalámbricas debido a las grandes oportunidades para la interceptación e inserción no detectadas en el tráfico de la red.

*Información adicional*
Las conexiones externas suministran un potencial para el acceso no autorizado a la información del negocio, por ejemplo el acceso a los métodos de marcación. Existen diferentes métodos de autenticación, algunos de los cuales proporcionan un mayor grado de protección que otros, como por ejemplo los métodos con base en el uso de técnicas criptográficas que pueden brindar autenticación sólida. Es importante determinar a partir de una evaluación de riesgos el grado necesario de protección. Ello es necesario para la selección adecuada de un método de autenticación.

Un medio para la conexión automática a un computador remoto podría suministrar una forma de obtener acceso no autorizado a una aplicación del negocio. Esto es especialmente importante si la conexión utiliza una red que está fuera del control de la gestión de la seguridad de la organización.

***11.4.3 Identificación de los equipos en las redes***

*Control*
La identificación automática de los equipos se debería considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.

*(Continúa)*

*Guía de implementación*
Se puede usar la identificación del equipo, si es importante que la comunicación únicamente se pueda iniciar desde un equipo o lugar específico. Un identificador en el equipo o acoplado a éste se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deberían indicar con claridad a qué red está permitido conectar el equipo, si existe más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesario considerar la protección física del equipo para mantener la seguridad del identificador de éste.

*Información adicional*
Este control se puede complementar con otras técnicas para autenticar el usuario del equipo (véase el numeral 11.4.2). La identificación del equipo se puede aplicar en adición a la autenticación del usuario.

***11.4.4 Protección de los puertos de configuración y diagnóstico remoto***

*Control*
El acceso lógico y físico a los puertos de configuración y de diagnóstico debería estar controlado.

*Guía de implementación*
Los controles potenciales para el acceso a los puertos de diagnóstico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnóstico y configuración sólo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar.

*Información adicional*
Muchos sistemas de computador, sistemas de red y sistemas de comunicación se instalan en un sitio de configuración o de diagnóstico remoto para ser utilizados por los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnóstico son un medio para el acceso no autorizado.

***11.4.5 Separación en las redes***

*Control*
En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información.

*Guía de implementación*
Un método para el control en las redes grandes es dividirlas en dominios lógicos de red separados, por ejemplo, dominios de red internos de la organización y dominios de red externos, cada uno protegido por un perímetro de la seguridad definido. Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aún más los entornos de la seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos. Los dominios se deberían definir con base en una evaluación de riesgos y en los diferentes requisitos de la seguridad en cada uno de los dominios.

Se puede implementar un perímetro de red instalando una puerta de enlace (*Gateway*) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (*Gateway*) se debería configurar para filtrar el tráfico entre estos dominios (véanse los numerales 11.4.6 y 11.4.7) y para bloquear el acceso no autorizado, según la política de control de acceso de la organización (véase el numeral 11.1). Un ejemplo de este tipo de puerta de enlace (*gateway*) es lo que se conoce comúnmente como barrera de fuego (*firewall*). Otro método para apartar los dominios lógicos separados es restringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro de la organización.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, por ejemplo la conmutación IP. Los dominios separados se pueden implementar entonces controlando los flujos de datos de la red usando las capacidades de enrutamiento / conmutación, como por ejemplo las listas de control de acceso.

*(Continúa)*

Los criterios para separar las redes en dominios se deberían basar en la política de control de acceso y en los requisitos de acceso (véase el numeral 10.1) y deberían tener en cuenta los costos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente de puerta de enlace (*Gateway*) o de enrutamiento de red (véanse los numerales 11.4.6 y 11.4.7).

Además, la separación de las redes se debería basar en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o los lineamientos del negocio con el fin de reducir el impacto total de una interrupción del servicio.

También se debería pensar en la separación de las redes inalámbricas procedentes de redes internas y privadas. Puesto que los perímetros de las redes inalámbricas no están bien definidos, es recomendable llevar a cabo una evaluación de riesgos en tales casos para identificar los controles (por ejemplo, autenticación sólida, métodos criptográficos y selección de frecuencia) para mantener la separación de la red.

*Información adicional*
Las redes se extienden cada vez más allá de las fronteras tradicionales de la organización, ya que se forman sociedades de negocios que pueden requerir la interconexión o compartir el procesamiento de información y las prestaciones de la red.

Tal extensión puede incrementar el riesgo no autorizado a los sistemas de información existentes que utilizan la red, algunos de los cuales pueden requerir protección contra otros usuarios de la red debido a su sensibilidad o importancia.

***11.4.6 Control de conexión a las redes***

*Control*
Para redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización, se debería restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio (véase el numeral 11.1).

*Guía de implementación*
Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso (véase el numeral 11.1.1).

La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (*gateway*) de red que filtren el tráfico por medio de tablas o reglas predefinidas.

Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

a) mensajería, por ejemplo, el correo electrónico;

b) transferencia de archivos;

c) acceso interactivo;

d) acceso a las aplicaciones.

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red con algunas horas del día o fechas.

*Información adicional*
La política de control del acceso puede exigir la incorporación de controles para restringir la capacidad de conexión de los usuarios a redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización.

*(Continúa)*

### *11.4.7 Control del enrutamiento en la red*

*Control*
Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

*Guía de implementación*
Los controles de enrutamiento se deberían basar en mecanismos de verificación para las direcciones fuente /destino válidos.

Las puertas de enlace (*Gateway*) de la seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa, si se emplean tecnologías *proxy* y/o de traducción de dirección de red. Quienes desarrollan la implementación deberían ser conscientes de las fortalezas y deficiencias de los mecanismos desplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en la política de control de acceso (véase el numeral 11.1).

*Información adicional*
Las redes compartidas, especialmente aquellas que van más allá de las fronteras de la organización, pueden requerir controles adicionales de enrutamiento. Esto se aplica particularmente cuando las redes son compartidas por usuarios de terceras partes (que no pertenecen a la organización).

## 11.5 Control de acceso al sistema operativo

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

Se recomienda utilizar medios de la seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

a) autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;

b) registrar intentos exitosos y fallidos de autenticación del sistema;

c) registrar el uso de privilegios especiales del sistema;

d) emitir alarmas cuando se violan las políticas de la seguridad del sistema;

e) suministrar medios adecuados para la autenticación;

f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

### *11.5.1 Procedimientos de registro de inicio seguro*

*Control*
El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.

*Guía de implementación*
El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) no mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente;

b) mostrar una advertencia de notificación general indicando que sólo deberían tener acceso al computador los usuarios autorizados;

*(Continúa)*

c) no suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado;

d) validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar qué parte de los datos es correcta o incorrecta;

e) limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar:

1) registrar intentos exitosos y fallidos;

2) forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica;

3) desconectar las conexiones de enlaces de datos;

4) enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio;

5) establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege;

f) limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación;

g) mostrar la siguiente información al terminar un registro de inicio exitoso:

1) fecha y hora del registro de inicio exitoso previo;

2) detalles de los intentos fallidos de registro de inicio desde el último registro exitoso;

h) no mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos;

i) no transmitir contraseñas en texto claro en la red.

*Información adicional*
Si las contraseñas se transmiten en texto claro durante la sesión de registro de inicio pueden ser capturadas en la red por un programa "husmeador" de red.

***11.5.2 Identificación y autenticación de usuarios***

*Control*
Todos los usuarios deberían tener un identificador único (ID del usuario) para su uso personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.

*Guía de implementación*
Este control se debería aplicar a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos).

Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona responsable. Las actividades de usuarios regulares no se deberían realizar desde cuentas privilegiadas.

En circunstancias excepcionales, cuando existe un beneficio claro para el negocio, se puede usar un identificador de usuario compartido para un grupo de usuarios o un trabajo específico.

La aprobación por la dirección debería estar documentada para dichos casos. Se pueden requerir controles adicionales para mantener la responsabilidad.

*(Continúa)*

Sólo se deberían permitir los identificadores (ID) de usuario genéricos para uso de un individuo si existen funciones accesibles o si no es necesario rastrear las acciones ejecutadas por el identificador (por ejemplo el acceso de sólo lectura), o cuando no hay controles establecidos (por ejemplo cuando la contraseña para un identificador genérico sólo se emite para un personal a la vez y el registro de tal caso).

Cuando se requiere verificación de identidad y autenticación sólidas, se deberían utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, *token* o medios biométricos.

*Información adicional*
Las contraseñas (véanse los numerales 11.3.1 y 11.5.3) son una forma muy común de identificar y autenticar con base en un secreto que sólo conoce el usuario. Lo mismo se puede lograr con medios criptográficos y protocolos de autenticación. La fortaleza de la identificación y autenticación del usuario debería ser adecuada a la sensibilidad de la información a la que se tiene acceso.

Objetos tales como los *tokens* de memoria o las tarjetas inteligentes que poseen los usuarios también se pueden usar para la identificación y la autenticación. Las tecnologías de autenticación biométrica que utilizan características o atributos únicos de un individuo también se pueden usar para autenticar la identidad de una persona. Una combinación de tecnologías y mecanismos enlazados con seguridad producirá una autenticación sólida.

***11.5.3 Sistema de gestión de contraseñas***

*Control*
Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

*Guía de implementación*
Un sistema de gestión de contraseñas debería:

a) hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad;

b) permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores en los ingresos;

c) imponer una elección de contraseñas de calidad (véase el numeral 11.3.1);

d) imponer cambios de contraseña (véase el numeral 11.3.1);

e) forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio (véase el numeral 11.2.3);

f) conservar un registro de las contraseñas de usuario previas y evitar su reutilización;

g) no mostrar contraseñas en la pantalla cuando se hace su ingreso;

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

i) almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo encriptadas o codificadas).

*Información adicional*
Las contraseñas son un mecanismo principal para validar una autoridad del usuario para tener acceso a un servicio de computador.

Algunas aplicaciones requieren la asignación de contraseñas de usuario por parte de una autoridad independiente, en tales casos, no se aplican los literales b), d) y e) indicados en la directriz anterior. En la mayoría de los casos, las contraseñas son seleccionadas y conservadas por los usuarios. Véase el numeral 11.3.1 para la directriz sobre el uso de contraseñas.

*(Continúa)*

### *11.5.4 Uso de las utilidades del sistema*

*Control*
Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

*Guía de aplicación*
Se recomienda considerar la siguiente directriz para el uso de las utilidades del sistema:

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

b) separación de las utilidades del sistema del software de aplicaciones,

c) limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados (véase el numeral 11.2.2);

d) autorización del uso ad hoc de las utilidades del sistema;

e) limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de un cambio autorizado;

f) registro de todo uso de las utilidades del sistema;

g) definición y documentación de los niveles de autorización para las utilidades del sistema;

h) retiro o inhabilitación de todas las utilidades o el software del sistema basado en software innecesario;

i) no poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.

*Información adicional*
La mayoría de las instalaciones de computador tiene uno o más programas de utilidades del sistema que pueden anular los controles del sistema y de la aplicación.

### *11.5.5 Tiempo de inactividad de la sesión*

*Control*
Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad.

*Guía de implementación*
Un tiempo de inactividad debería despejar la pantalla de sesión y más tarde, cerrar tanto la sesión de la aplicación como la de red después de un periodo definido de inactividad. La dilación del tiempo de inactividad debería reflejar los riesgos de la seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo.

Algunos sistemas pueden suministrar una forma limitada de utilidad de tiempo de inactividad la cual despeja la pantalla y evita el acceso no autorizado, pero no cierra las sesiones de aplicación ni de red.

*Información adicional*
Este control es importante particularmente en lugares de alto riesgo, los cuales incluyen áreas públicas o externas fuera de la gestión de la seguridad de la organización. Las sesiones se deberían cerrar para evitar el acceso de personas no autorizadas y negar ataques al servicio.

### *11.5.6 Limitación del tiempo de conexión*

*Control*
Se deberían utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

*(Continúa)*

*Guía de implementación*
Se deberían tener en cuenta los controles de tiempo para las aplicaciones sensibles de computador, especialmente las de lugares de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la gestión de la seguridad de la organización. Los siguientes son algunos ejemplos de estas restricciones:

a) uso de espacios de tiempo predeterminados, por ejemplo, para transmisiones de lotes de archivos, o uso de sesiones interactivas de corta duración;

b) restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado;

c) considerar la repetición de la autenticación a intervalos determinados.

*Información adicional*
La limitación del periodo durante el cual se permite la conexión a los servicios de computador reduce la ventana de oportunidad para el acceso no autorizado. La limitación de la duración de las sesiones activas evita que los usuarios mantengan sesiones abiertas para evitar la repetición de la autenticación.

## 11.6 Control de acceso a las aplicaciones y a la información

**Objetivo:** evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.

Se deberían usar medios de la seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.

El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados.

Los sistemas de aplicación deberían:

a) controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;

b) suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación;

c) no poner en peligro otros sistemas con los que se comparten los recursos de información.

### *11.6.1 Restricción del acceso a la información*

*Control*
Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

*Guía de implementación*
Las restricciones del acceso se deberían basar en los requisitos de las aplicaciones individuales del negocio. La política de control de acceso también debería ser consistente con la política de acceso de la organización (véase el numeral 11.1).

Se debería considerar la aplicación de las siguientes directrices con el objeto de dar soporte a los requisitos de restricción del acceso:

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

b) controlar los derechos de acceso de los usuarios, por ejemplo, leer, escribir, eliminar y ejecutar;

c) controlar los derechos de acceso de otras aplicaciones;

*(Continúa)*

d) garantizar que los datos de salida de los sistemas de aplicación que manejan información sensible sólo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados; ello debería incluir revisiones periódicas de dichas salidas para garantizar el retiro de la información redundante.

### *11.6.2 Aislamiento de sistemas sensibles*

*Control*
Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

*Guía de implementación*
Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) la sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del responsable de la aplicación (véase el numeral 7.1.2);

b) cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados por el responsable de la aplicación sensible.

*Información adicional*
Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicar que el sistema de aplicación debería:

a) ejecutarse en un computador dedicado, o

b) únicamente debería compartir recursos con sistemas de aplicación confiables.

El aislamiento se puede lograr utilizando métodos físicos o lógicos (véase el numeral 11.4.5).

## 11.7 Computación móvil y trabajo remoto

**Objetivo:** garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.

La protección necesaria debería estar acorde con los riesgos que originan estas formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada. En el caso del trabajo remoto, la organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

### *11.7.1 Computación y comunicaciones móviles*

*Control*
Se debería establecer una política formal y se deberían adoptar las medidas de la seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

*Guía de implementación*
Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (*Notebooks*), microcomputadores de bolsillo (*Palmtops*), y computadores portátiles pesados (*Laptops*), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos sin protección.

*(Continúa)*

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas (véase el numeral 12.3).

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado, para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizados (véase el numeral 10.4).

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio.

Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información.

Las copias de respaldo deberían tener protección adecuada contra robo o pérdida de información.

La utilización de los servicios móviles conectados a las redes deberían tener una protección idónea. El acceso remoto a la información del negocio a través de redes públicas usando servicios de computación móvil sólo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuados de control del acceso (véase el numeral 11.4). Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centros de conferencias y sitios de reuniones.

Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de la seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil. El equipo que porta información sensible y / o crítica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo (véase el numeral 9.2.5).

Se recomienda disponer la formación del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

*Información adicional*
Las conexiones inalámbricas a red móvil son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se deberían considerar al identificar los controles. Las diferencias típicas son:

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

b) la información almacenada en los computadores móviles puede no tener copias de respaldo debido al ancho de banda de red limitado y / o a que el equipo móvil puede no estar conectado en las horas en las que están programadas las copias de respaldo.

### *11.7.2 Trabajo remoto*

*Control*
Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

*Guía de implementación*
Las organizaciones sólo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de la seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de la seguridad de la organización.

*(Continúa)*

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo, robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) la seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local;

b) el entorno físico de trabajo remoto propuesto;

c) los requisitos de la seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno;

d) la amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos;

e) el uso de redes domésticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica;

f) las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada;

g) el acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley;

h) los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o usuarios de terceras partes;

i) protección antivirus y requisitos de barreras contra fuego (firewall).

Las directrices y disposiciones a considerar deberían incluir las siguientes:

a) disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no esté bajo el control de la organización;

b) definición del trabajo que se permite realizar, las horas laborables, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado;

c) disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto;

d) seguridad física;

e) reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información;

f) disposición de soporte y mantenimiento de hardware y software;

g) disposición de pólizas de seguros;

h) procedimientos para el respaldo y la continuidad del negocio;

i) auditoría y monitoreo de la seguridad;

*(Continúa)*

j) revocación de autoridad y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.

*Información adicional*
En el trabajo remoto se emplean tecnologías de comunicaciones que le permiten al personal realizar trabajo remoto desde un lugar fijo fuera de su organización.

# 12. Adquisición, desarrollo y mantenimiento de sistemas de información

## 12.1 Requisitos de la seguridad de los sistemas de información

Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Se deberían identificar y acordar los requisitos de la seguridad antes del desarrollo y / o la implementación de los sistemas de información.

Todos los requisitos de la seguridad se deberían identificar en la fase de requisitos de un proyecto y se deberían justificar, acordar y documentar como parte de todo el caso del negocio para un sistema de información.

### *12.1.1 Análisis y especificación de los requisitos de la seguridad*

*Control*
Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de la seguridad.

*Guía de implementación*
En las especificaciones para los requisitos de control se deberían considerar los controles automatizados que se han de incorporar en el sistema de información y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares al evaluar los paquetes de software, desarrollados o adquiridos, para las aplicaciones del negocio.

Los requisitos de la seguridad y los controles deberían reflejar el valor para el negocio de los activos de información involucrados (véase el numeral 7.2) y el daño potencial para el negocio que se puede presentar debido a falla o ausencia de la seguridad.

Los requisitos del sistema para la seguridad de la información y los procesos para implementarla se deberían integrar en las fases iniciales de los proyectos del sistema de información. Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Si se adquieren productos, se debería seguir un proceso formal de adquisición y prueba.

Los contratos con el proveedor deberían abordar los requisitos de la seguridad identificados.

Cuando la funcionalidad de la seguridad de un producto determinado no satisface el requisito específico, entonces es conveniente considerar los controles de los riesgos, introducidos y asociados, antes de adquirir el producto. Cuando se proporciona funcionalidad adicional y ello causa un riesgo de la seguridad, tal funcionalidad se debería inhabilitar o se debería revisar la estructura del control propuesto para determinar si se puede obtener ventaja de la funcionalidad mejorada disponible.

*Información adicional*
Si se considera apropiado, por ejemplo por razones de costos, la dirección podría utilizar productos certificados y evaluados independientemente. Información adicional sobre los criterios para los productos de la seguridad de la tecnología de la información se puede encontrar en la norma ISO/IEC 15408 o en otras normas sobre evaluación y certificación, según sea apropiado.

*(Continúa)*

La norma ISO/IEC TR 13335-3 proporciona directrices sobre el uso de procesos de gestión de riesgos para identificar los requisitos de los controles de la seguridad.

## 12.2 Procesamiento correcto en las aplicaciones

**Objetivo:** evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

Se deberían diseñar controles apropiados en las aplicaciones, incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada, del procesamiento interno y de los datos de salida.

Se pueden necesitar controles adicionales para los sistemas que procesan o tienen impacto en la información sensible, de valor o crítica. Dichos controles se deberían determinar con base en los requisitos de la seguridad y en una evaluación de riesgos.

### *12.2.1 Validación de los datos de entrada*

*Control*
Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

*Guía de implementación*

Es recomendable realizar verificaciones de las entradas de las transacciones del negocio, de los datos permanentes (por ejemplo, nombres y direcciones, límites de crédito, números de referencia del cliente) y de las tablas de parámetros ( por ejemplo, precios de venta, tasas de conversión de divisas, tasas de impuestos). Se recomienda tomar en consideración las siguientes directrices:

a) verificaciones de entradas duales u otras entradas, tales como verificación de fronteras o campos limitantes para especificar los rangos de los datos de entrada, con el fin de detectar los siguientes errores:

   1) valores fuera de rango;

   2) caracteres no válidos en los campos de datos;

   3) datos incompletos o ausentes;

   4) exceso en los límites superiores e inferiores del volumen de datos;

   5) datos de controles inconsistentes o no autorizados;

b) revisión periódica del contenido de los campos clave o de los archivos de datos para confirmar su validez e integridad;

c) inspección de los documentos de entrada impresos para determinar cambios no autorizados (todos los cambios en los datos de entrada deben estar autorizados);

d) procedimientos de respuesta ante errores de validación;

e) procedimientos para probar la credibilidad de los datos de entrada;

f) definición de responsabilidades para todo el personal que participa en el proceso de entrada de datos;

g) creación de un registro de las actividades implicadas en el proceso de entrada de datos (véase el numeral 10.10.1).

*(Continúa)*

*Información adicional*
Se recomienda la inspección y la validación automática de los datos de entrada, cuando se puedan aplicar, para reducir el riesgo de errores y evitar ataques normales, incluyendo desbordamiento de búfer o inyección de códigos.

***12.2.2 Control de procesamiento interno***

*Control*
Se deberían incorporar verificaciones de validación en las aplicaciones para detectar cualquier daño o pérdida de la información por errores de procesamiento o actos deliberados.

*Guía de implementación*
El diseño y la implementación de las aplicaciones deberían garantizar que se minimizan los riesgos de falla en el procesamiento, los cuales originan pérdida de la integridad. Las áreas específicas que se han de considerar incluyen:

a) utilización de las funciones agregar, modificar y borrar para implementar los cambios en los datos;

b) procedimientos para evitar que los programas se ejecuten en orden erróneo o su ejecución después de una falla previa del procesamiento (véase el numeral 10.1.1);

c) utilización de programas adecuados para la recuperación después de fallas con el fin de garantizar el procesamiento correcto de los datos;

d) protección contra ataques empleando desbordamiento / exceso en el búfer.

Se deberían elaborar listas de verificación adecuadas, documentar las actividades y mantener seguros los resultados. Los siguientes son algunos ejemplos de verificaciones que se pueden incorporar:

a) controles de sesión o de lotes, para conciliar los balances de archivos de datos después de actualizar las transacciones;

b) controles de balance, para verificar los balances de apertura frente a los balances de cierre previos, tales como:

   1) controles para cada ejecución;

   2) totales de actualizaciones de archivos;

   3) controles programa a programa;

c) validación de los datos de entrada generados por el sistema (véase el numeral 12.2.1);

d) verificaciones de la integridad, la autenticidad o cualquier otra característica de seguridad de los datos o del software descargado o actualizado entre el computador central y el remoto;

e) totales de verificación (*hash*) de registros y archivos;

f) verificaciones para garantizar que los programas de aplicación se ejecutan en el momento correcto;

g) verificaciones para garantizar que los programas se ejecutan en el orden correcto y finalizan en caso de falla, y que el procesamiento posterior se detiene hasta resolver el problema;

h) creación de un registro de las actividades implicadas en el procesamiento (véase el numeral 10.10.1).

*Información adicional*
Los datos que se han ingresado correctamente se pueden corromper por errores de software, errores de procesamiento o a través de actos deliberados. Las verificaciones de validación requeridas dependerán de la naturaleza de la aplicación y del impacto de la corrupción de los datos en el negocio.

*(Continúa)*

### *12.2.3 Integridad del mensaje*

*Control*
Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

*Guía de implementación*
Se debería realizar una evaluación de los riesgos de la seguridad para determinar si se requiere integridad del mensaje y para identificar el método más apropiado de implementación.

*Información adicional*
Se pueden usar las técnicas criptográficas (véase el numeral 12.3) como un medio apropiado para implementar la autenticación del mensaje.

### *12.2.4 Validación de los datos de salida*

*Control*
Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.

*Guía de implementación*
La validación de los datos de salida puede incluir:

a) verificaciones de la verosimilitud para probar si los datos de salida son razonables;

b) cuentas de control de conciliación para asegurar el procesamiento de todos los datos;

c) suministro de información suficiente para que un lector o un sistema de procesamiento posterior determine la exactitud, totalidad, precisión y clasificación de la información;

d) procedimientos para responder las pruebas de validación de salidas;

e) definición de las responsabilidades de todo el personal que participa en el proceso de la salida de datos;

f) creación de un registro de las actividades del proceso de validación de la salida de datos.

*Información adicional*
Comúnmente, los sistemas y las aplicaciones se construyen asumiendo que al realizar la validación, la verificación y las pruebas adecuadas, la salida siempre será correcta. Sin embargo, esta suposición no siempre es válida; es decir, los sistemas que se han sometido a prueba aún pueden producir salidas incorrectas en algunas circunstancias.

## 12.3 Controles criptográficos

**Objetivo:** proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.

Se debería desarrollar una política sobre el uso de los controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.

### *12.3.1 Política 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.

*Guía de implementación*
Se recomienda tomar en consideración los siguientes aspectos al desarrollar una política criptográfica:

*(Continúa)*

a) el enfoque de la dirección hacia el uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se debería proteger la información del negocio (véase el numeral 5.1.1);

b) con base en una evaluación de riesgos, se debería identificar el nivel requerido de protección teniendo en cuenta tipo, fortaleza y calidad del algoritmo de encriptación requerido;

c) uso de encriptación para la protección de la información sensible transportada por medios móviles o removibles, por dispositivos o a través de las líneas de comunicación;

d) enfoque para la gestión de claves, incluyendo los métodos para tratar la protección de las claves criptográficas y la recuperación de información encriptada en caso de pérdida, amenaza o daño de las claves;

e) funciones y responsabilidades, por ejemplo, quién es responsable de:

1) la implementación de la política;

2) la gestión de claves, incluyendo su generación (véase el numeral 12.3.2);

f) normas que se han de adoptar para la implementación eficaz en toda la organización (qué solución se usa para cuáles procesos del negocio);

g) impacto de la utilización de información encriptada sobre los controles que depende de la inspección del contenido (por ejemplo, detección de virus).

Cuando se implementa la política de encriptación de la organización, es conveniente tener en mente los reglamentos y las restricciones nacionales que se pueden aplicar al uso de técnicas criptográficas en diferentes partes del mundo y los aspectos del flujo trans-fronterizo de información encriptada (véase el numeral 15.1.6).

Los controles criptográficos se pueden utilizar para lograr diferentes objetivos de la seguridad, por ejemplo:

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

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

c) no-repudio: uso de técnicas criptográficas para obtener prueba de la ocurrencia o no ocurrencia de un evento o acción.

*Información adicional*

La decisión sobre la idoneidad de la solución criptográfica debería formar parte del proceso más amplio de evaluación de riesgos y selección de controles. Esta evaluación se puede usar para determinar si un control criptográfico es adecuado, el tipo de control que se debería aplicar y para qué propósito y cuál proceso del negocio.

La política sobre el empleo de controles criptográficos es necesaria para maximizar los beneficios y minimizar los riesgos de usar las técnicas criptográficas, y para evitar el uso incorrecto o inapropiado. Cuando se utilizan firmas digitales, se recomienda considerar toda la legislación pertinente, en particular la legislación que describe las condiciones bajo las cuales la firma digital es legalmente obligatoria (véase el numeral 15.1).

Es conveniente buscar asesoría especializada para identificar el nivel apropiado de protección y definir las especificaciones adecuadas que suministrarán la protección requerida y el soporte a la implementación de un sistema seguro de gestión de claves (véase el numeral 12.3.2).

El comité ISO/IEC JTC1 SC27 ha desarrollado varias normas relacionadas con los controles criptográficos. Información adicional se puede encontrar en la norma IEEE P1363 y en las directrices OECD sobre criptografía.

*(Continúa)*

### *12.3.2 Gestión de claves*

*Control*
Se debería establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización.

*Guía de implementación*
Todas las claves criptográficas deberían tener protección contra modificación, pérdida y destrucción. Además, las claves privadas y secretas necesitan protección contra divulgación no autorizada. El equipo usado para generar, almacenar y archivar las claves debería estar protegido por medios físicos.

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

a) generar claves para diferentes sistemas criptográficos y diferentes aplicaciones;

b) generar y obtener certificados de claves públicas;

c) distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves;

d) almacenar las claves, incluyendo la forma en que los usuarios autorizados tendrán acceso a ellas;

e) cambiar o actualizar las claves incluyendo reglas sobre cuándo cambiarlas y cómo hacerlo;

f) tratar las claves perdidas;

g) revocar las claves, incluyendo la forma de retirarlas o desactivarlas, por ejemplo, cuando las claves se han puesto en peligro o cuando un usuario se retira de la organización (en cuyo caso las claves también se deberían archivar);

h) recuperar claves pérdidas o corruptas como parte de la gestión de continuidad del negocio; por ejemplo, para la recuperación de información encriptada;

i) archivar claves, por ejemplo para la información archivada o con copia de respaldo;

j) destrucción de claves;

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

Para reducir la probabilidad de poner en peligro, activar o desactivar se deberían definir fechas para las claves de modo que sólo se puedan utilizar durante un periodo de tiempo limitado.

Este período dependería de las circunstancias en las cuales se usa el control criptográfico y del riesgo percibido.

Además de las claves privadas y secretas con gestión segura, también se debería pensar en la autenticidad de las claves públicas. Este proceso de autenticación se puede hacer con certificados de claves públicas que normalmente son emitidos por una autoridad de certificación, la cual debe ser una organización reconocida con controles y procedimientos idóneos establecidos para proporcionar el grado requerido de confianza.

El contenido de los acuerdos o contratos de servicios con proveedores externos de servicios criptográficos, por ejemplo con una autoridad de certificación, deberían comprender aspectos de responsabilidad, confiabilidad de los servicios y tiempos de respuesta para la prestación de los servicios (véase el numeral 6.2.3).

*Información adicional*
La gestión de las claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. La norma ISO/IEC 11770 brinda información adicional sobre la gestión de claves. Los dos tipos de técnicas criptográficas son:

*(Continúa)*

a) técnicas de clave secreta, en donde dos o más partes comparten la misma clave y ésta se usa tanto para encriptar como desencriptar información; esta clave debe mantenerse secreta puesto que cualquiera que tenga acceso a ella puede descifrar toda la información encriptada con dicha clave, o introducir información no autorizada con esa clave;

b) técnicas de clave pública, en donde cada usuario tiene un par de claves, una clave pública (que se puede revelar a cualquiera) y una clave privada (que se debe mantener en secreto); las técnicas de clave pública se pueden usar para la encriptación y para producir firmas digitales (véase la norma ISO/IEC 9 796 e ISO/IEC 14 888).

Existe una amenaza de falsificar una firma digital reemplazando la clave pública del usuario. Este problema se puede tratar usando un certificado de clave pública.

Las técnicas criptográficas también se pueden usar para proteger las claves criptográficas. Es necesario que en los procedimientos se considere el manejo de solicitudes legales para acceder a las claves criptográficas, por ejemplo, puede ser necesario poner a disposición la información encriptada en un formato sin encriptación como evidencia en caso de un juicio.

## 12.4 Seguridad de los archivos del sistema

| |
|---|
| Objetivo: garantizar la seguridad de los archivos del sistema.<br><br>Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos, y los proyectos de tecnología de la información y las actividades de soporte se deberían efectuar de forma segura. Se debería tener cuidado para evitar la exposición de datos sensibles en los entornos de prueba. |

### *12.4.1 Control del software operativo*

*Control*
Se deberían establecer procedimientos para controlar la instalación de software en los sistemas operativos.

*Guía de implementación*
Para minimizar los riesgos de corrupción de los sistemas operativos, se deberían tener en cuenta las siguientes directrices para controlar los cambios:

a) la actualización del software operativo, las aplicaciones y las bibliotecas de los programas sólo deberían ser realizadas por administradores capacitados y con la debida autorización de la dirección (véase el numeral 12.4.3);

b) los sistemas operativos únicamente deberían contener códigos ejecutables aprobados y no códigos en desarrollo ni compiladores;

c) el software de las aplicaciones y del sistema operativo sólo se deberían implementar después del ensayo exhaustivo y exitoso; los ensayos deberían incluir pruebas sobre capacidad de uso, seguridad, efectos en otros sistemas y facilidad para el usuario, igualmente se deberían efectuar en sistemas separados (véase el numeral 10.1.4); se debería garantizar que todas las bibliotecas fuente del programa correspondiente estén actualizadas;

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

e) es conveniente implantar una política de estrategia de restauración al estado anterior antes de implementar los cambios;

f) se debería conservar un registro para auditoría de todas las actualizaciones de las bibliotecas de los programas operativos;

g) es conveniente conservar las versiones anteriores del software de aplicación como medida de contingencia;

*(Continúa)*

h) las versiones antiguas del software se deberían archivar junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte, en la medida en que los datos se retengan en archivo.

El software suministrado por el vendedor utilizado en los sistemas operativos se debería mantener en el nivel con soporte del proveedor. Con el tiempo, los vendedores de software dejarán de dar soporte a las versiones antiguas del software. La organización debería considerar los riesgos de depender de software sin soporte.

En toda decisión para mejorar a una nueva versión se debería contar con los requisitos del negocio para el cambio, y la seguridad de la nueva versión, es decir, la introducción de nueva funcionalidad en el sistema o la cantidad y gravedad de los problemas de seguridad que afectan a esta versión. Los parches de software se deberían aplicar cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad (véase el numeral 12.6.1).

El acceso físico o lógico únicamente se debería dar a los proveedores para propósitos de soporte, cuando sea necesario, y con aprobación de la dirección. Las actividades del proveedor se deberían monitorear.

El software del computador puede depender de software y módulos suministrados externamente, lo cual se debería monitorear y controlar para evitar cambios no autorizados que puedan introducir debilidades de seguridad.

*Información adicional*
Los sistemas operativos únicamente se deberían mejorar cuando existe una necesidad para hacerlo, por ejemplo, si la versión actual del sistema operativo ya no da soporte a los requerimientos del negocio. Las mejoras no deberían tener lugar sólo porque esté disponible una nueva versión del sistema operativo. Las versiones nuevas del sistema operativo pueden ser menos seguras, menos estables, y menos entendidas que los sistemas actuales.

### *12.4.2 Protección de los datos de prueba del sistema*

*Control*
Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

*Guía de implementación*
Se debería evitar el uso de bases de datos operativos que contienen información personal o cualquier otra información sensible con propósitos de prueba. Si se utiliza información personal o de otra forma sensible para propósitos de prueba, todos los detalles y el contenido sensible se deberían retirar o modificar antes del uso para evitar el reconocimiento. Las siguientes directrices se deberían aplicar para proteger los datos operativos cuando se emplean con propósitos de prueba:

a) los procedimientos de control del acceso que se aplican a los sistemas de aplicación operativos también se deberían aplicar a los sistemas de aplicación de pruebas;

b) debería existir autorización separada cada vez que se copia la información operativa en un sistema de aplicación de prueba;

c) la información operativa se debería borrar del sistema de aplicación de prueba inmediatamente después de terminar la prueba;

d) el copiado y utilización de la información operativa se debería registrar para brindar un rastro para auditoría.

*Información adicional*
La prueba del sistema y de aceptación usualmente exige volúmenes sustanciales de datos de prueba que sean lo más cercanos posible a los datos operativos.

### *12.4.3 Control de acceso al código fuente de los programas*

*Control*
Se debería restringir el acceso al código fuente de los programas.

*(Continúa)*

*Guía de implementación*
El acceso al código fuente de programas y a los elementos asociados (como diseños, especificaciones, planes de verificación y planes de validación) se debería controlar estrictamente para evitar la introducción de funcionalidad no autorizada y evitar los cambios involuntarios. Para el código fuente de programas esto se puede lograr con el almacenamiento central controlado de dicho código, preferiblemente en las bibliotecas fuente de programas. Las siguientes directrices se deberían considerar (véase el numeral 11) para controlar el acceso a tales bibliotecas fuente de programas, con el objeto de reducir el potencial de corrupción de los programas del computador:

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

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

c) el personal de soporte debería tener acceso restringido a las bibliotecas fuente de programas;

d) la actualización de las bibliotecas fuente de programas y de los elementos asociados, así como la emisión de fuentes de programa a los programadores, solamente se debería efectuar después de recibir la autorización apropiada;

e) los listados de programas se deberían mantener en un entorno seguro (véase el numeral 10.7.4);

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

g) el mantenimiento y el copiado de las bibliotecas fuente de programas deberían estar sujetos a un procedimiento estricto de control de cambios (véase el numeral 12.5.1).

*Información adicional*
El código fuente de programas es un código escrito por los programadores, el cual está compilado (y enlazado) para crear ejecutables. Algunos lenguajes de programación no distinguen formalmente entre el código fuente y los ejecutables ya que estos últimos se crean en el momento en que se activan.

Las normas ISO 10 007 and ISO/IEC 12 207 brindan información adicional sobre la gestión de la configuración y el proceso del ciclo de vida del software.

## 12.5 Seguridad en los procesos de desarrollo y soporte

Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.

Los entornos de soporte y de desarrollo deberían estar estrictamente controlados.

Los directores responsables de los sistemas de aplicación también deberían ser responsables de la seguridad del entorno del proyecto o del soporte. Ellos deberían garantizar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del entorno operativo.

### *12.5.1 Procedimientos de control de cambios*

*Control*
Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

*Guía de implementación*
Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para minimizar la corrupción de los sistemas de información. La introducción de sistemas nuevos y de cambios importantes en los sistemas existentes debería seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación con gestión.

*(Continúa)*

Este proceso debería incluir una evaluación de riesgos, análisis de los impactos de los cambios y especificación de los controles de seguridad necesarios. Este proceso también debería garantizar que la seguridad y los procesos de control existentes no se ponen en peligro, que se da acceso a los programadores de soporte sólo a aquellas partes del sistema necesarias para su trabajo y que existe acuerdo y aprobación formal para cualquier cambio.

Siempre que sea factible, los procedimientos de control de cambios operativos y de aplicación se deberían integrar (véase el numeral 10.1.2). Los procedimientos de control de cambios deberían incluir:

a) el mantenimiento de un registro de los niveles acordados de autorización;

b) la garantía de que los cambios son realizados por los usuarios autorizados;

c) la revisión de los controles y de los procedimientos de integridad para asegurar que no se pondrán en peligro debido a los cambios;

d) la identificación de todo el software, la información, las entidades de bases de datos y del hardware que requieran mejora;

e) la obtención de la aprobación formal de las propuestas detalladas antes de iniciar el trabajo;

f) la garantía de que los usuarios autorizados aceptan los cambios antes de la implementación;

g) la garantía de que la documentación del sistema está actualizada al finalizar cada cambio y que la documentación antigua se archiva o elimina;

h) el mantenimiento de una versión de control para todas las actualizaciones de software;

i) el mantenimiento de un rastro para auditoría de todos los cambios solicitados;

j) la garantía de que la documentación operativa (véase el numeral 10.1.1) y los procedimientos de usuario se cambian en función de la necesidad con el objeto de mantener su idoneidad;

k) la garantía de que la implementación de los cambios tiene lugar en el momento oportuno y no perturba los procesos del negocio involucrados.

*Información adicional*
El cambio del software puede tener impacto en el entorno operativo.

Una buena práctica incluye la prueba del software nuevo en un entorno separado tanto del entorno de producción como del de desarrollo (véase el numeral 10.1.4). Esto proporciona medios para controlar el software nuevo y facilitar la protección adicional de la información operativa que se usa con propósitos de prueba. Se deberían incluir parches, paquetes de servicio y otras actualizaciones. Las actualizaciones automáticas no se deberían utilizar en sistemas críticos ya que algunas de ellas pueden causar fallas de las aplicaciones críticas (véase el numeral 12.6).

***12.5.2 Revisión técnica de las aplicaciones después de los cambios en el sistema operativo***

*Control*
Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

*Guía de implementación*
Este proceso debería comprender los siguientes aspectos:

a) revisión de los procedimientos de integridad y control de la aplicación para asegurarse de que no se han puesto en peligro debido a los cambios en el sistema operativo;

b) garantía de que el plan y el presupuesto de soporte anual cubrirán las revisiones y pruebas del sistema que resulten de cambios en el sistema operativo;

*(Continúa)*

c) garantía de la notificación oportuna sobre los cambios en el sistema operativo para permitir la realización de las pruebas y las revisiones apropiadas antes de la implementación;

d) garantía de que se hacen cambios en los planes de continuidad del negocio (véase el numeral 14).

Un grupo o un individuo específico debería ser responsable de monitorear las vulnerabilidades y las nuevas versiones de parches y arreglos (*fixes*) del distribuidor (véase el numeral 12.6).

### *12.5.3 Restricciones en los cambios a los paquetes de software*

*Control*
Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

*Guía de implementación*
En la medida de lo posible y viable, los paquetes de software suministrados por el vendedor se deberían usar sin modificaciones. Cuando sea necesario modificar un paquete de software, se deberían tener en cuenta los siguientes puntos:

a) el riesgo de que los procesos de integridad y de control incorporados se vean comprometidos;

b) si es necesario obtener el consentimiento del vendedor;

c) la posibilidad de obtener los cambios requeridos del vendedor como un programa estándar de actualizaciones;

d) el impacto, si la organización se hace responsable del mantenimiento futuro del software como resultado de los cambios.

Si los cambios son necesarios, el software original se debería conservar y los cambios se deberían aplicar a una copia claramente identificada. Se debería implementar un proceso de gestión de las actualizaciones del software para asegurarse de que los parches más actualizados aprobados y las actualizaciones de las aplicaciones están instalados en todo el software autorizado (véase el numeral 12.6). Todos los cambios se deberían probar y documentar en su totalidad de manera que se puedan volver a aplicar, si es necesario, para mejoras futuras del software. Si así se requiere, las modificaciones se deberían probar y validar por un organismo de evaluación independiente.

### *12.5.4 Fuga de información*

*Control*
Se deberían evitar las oportunidades para que se produzca fuga de información.

*Guía de implementación*
Se deberían considerar los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos:

a) exploración de los medios y comunicaciones de salida para determinar la información oculta;

b) comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento;

c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408);

d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes;

e) monitoreo del uso de los recursos en los sistemas de computador.

*(Continúa)*

*Información adicional*
Los canales encubiertos son vías que no están destinadas para conducir flujos de información, pero que, sin embargo, pueden existir en un sistema o una red. Por ejemplo, los bits de manipulación en los paquetes de protocolo de comunicaciones se podrían usar como un método oculto de señalización. Debido a su naturaleza, evitar la existencia de todos los posibles canales encubiertos sería difícil, si no imposible. No obstante, la explotación de tales canales se realiza con frecuencia a través de códigos troyanos (véase el numeral 10.4.1). Por lo tanto, tomar medidas para proteger contra códigos troyanos reduce el riesgo de explotación de los canales encubiertos.

La prevención del acceso no autorizado a la red (véase el numeral 11.4), así como las políticas y los procedimientos para desalentar el uso inadecuado de los servicios de información por parte del personal (véase el numeral 15.1.5) facilitarán la protección contra canales encubiertos.

### *12.5.5 Desarrollo de software contratado externamente*

*Control*
La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

*Guía de implementación*
Cuando el desarrollo del software se contrata externamente, se recomienda tener en cuenta los siguientes puntos:

a) acuerdos sobre licencias, propiedad de los códigos y derechos de propiedad intelectual (véase el numeral 15.1.2);

b) certificación de la calidad y exactitud del trabajo realizado;

c) convenios de fideicomiso en caso de falla de la tercera parte;

d) derechos de acceso para auditar la calidad y exactitud del trabajo realizado;

e) requisitos contractuales para la calidad y la funcionalidad de la seguridad del código;

f) realización de pruebas antes de la instalación para detectar códigos troyanos o maliciosos.

## 12.6 Gestión de la vulnerabilidad técnica

Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica se debería implementar de forma eficaz, sistemática y repetible con toma de mediciones para confirmar su eficacia. Estas consideraciones deberían incluir a los sistemas operativos y otras aplicaciones en uso.

### *12.6.1 Control de las vulnerabilidades técnicas*

*Control*
Se debería obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

*Guía de implementación*
Un inventario completo y actual de los activos (véase el numeral 7.1) es un prerrequisito para la gestión eficaz de la vulnerabilidad técnica. La información específica necesaria para dar soporte a la gestión de la vulnerabilidad técnica incluye los siguientes datos: vendedor del software, números de versión, estado actual de despliegue (por ejemplo qué software está instalado en cuál sistema) y las personas de la organización responsables del software.

Es conveniente tomar la acción oportuna y apropiada en respuesta a la identificación de vulnerabilidades técnicas potenciales. Se recomienda tener en cuenta las siguientes directrices para establecer un proceso de gestión eficaz de las vulnerabilidades técnicas:

*(Continúa)*

a) la organización debería definir e instaurar las funciones y responsabilidades asociadas con la gestión de la vulnerabilidad técnica, incluyendo el monitoreo de la vulnerabilidad, la evaluación de riesgos de la vulnerabilidad, el uso de parches, el rastreo de activos y todas las responsabilidades de coordinación requeridas;

b) es conveniente identificar los recursos de información que se van a utilizar para identificar las vulnerabilidades técnicas pertinentes y para mantener la concientización sobre ellas para el software y otra tecnología (con base en la lista de inventario de activos, véase el numeral 7.1.1), estos recursos de información se deberían actualizar en función de los cambios en el inventario o cuando se encuentran recursos nuevos o útiles;

c) se debería definir una línea de tiempo para reaccionar ante la notificación de vulnerabilidades técnicas potenciales pertinentes;

d) una vez se ha identificado una vulnerabilidad potencial, la organización debería identificar los riesgos asociados y las acciones que se han de tomar; tales acciones podrían involucrar el uso de parches en los sistemas vulnerables y / o la aplicación de otros controles;

e) dependiendo de la urgencia con la que es necesario tratar la vulnerabilidad técnica, la acción a tomar se debería ejecutar de acuerdo con los controles relacionados con la gestión de cambios (véase el numeral 12.5.1) o siguiendo los procedimientos de respuesta ante incidentes de seguridad de la información;

f) si está disponible un parche, se deberían evaluar los riesgos asociados con su instalación (los riesgos impuestos por la vulnerabilidad se deberían comparar con los riesgos de instalar el parche);

g) es conveniente probar y evaluar los parches antes de su instalación para garantizar que son eficaces y no producen efectos secundarios intolerables; si no hay parche disponible, se recomienda considerar otros controles:

   1) apagar los servicios o capacidades relacionadas con la vulnerabilidad;

   2) adaptar o agregar controles de acceso, por ejemplo, barreras de fuego (*firewalls*), en las fronteras de la red (véase el numeral 11.4.5);

   3) aumentar el monitoreo para detectar o prevenir los ataques reales;

   4) crear conciencia sobre la vulnerabilidad;

h) se debería conservar un registro para auditoría para todos los procedimientos efectuados;

i) el proceso de gestión de la vulnerabilidad técnica se debería monitorear y evaluar a intervalos regulares para garantizar su eficacia y eficiencia;

j) se deberían tratar primero los sistemas con alto riesgo.

*Información adicional*

El funcionamiento correcto del proceso de gestión de la vulnerabilidad técnica es crítico para muchas organizaciones y por ello se debería monitorear con regularidad. Es esencial un inventario exacto para garantizar la identificación de vulnerabilidades técnicas potenciales y pertinentes.

La gestión de la vulnerabilidad técnica se puede ver como una sub-función de la gestión de cambios y como tal puede tomar ventaja de los procesos y procedimientos de gestión de cambios (véanse los numerales 10.1.2 y 12.5.1).

Los vendedores, con frecuencia, están bajo gran presión para sacar a la venta los parches tan pronto sea posible. Por lo tanto, es posible que un parche no trate el problema adecuadamente y tenga efectos colaterales negativos. En algunos casos, desinstalar un parche puede no ser tan fácil una vez que se ha aplicado.

Si no es posible someter los parches a las pruebas adecuadas, por ejemplo, debido a los costos o a la falta de recursos, se puede pensar en retrasar la aplicación del parche para valorar los riesgos asociados, basados en la experiencia reportada por otros usuarios.

*(Continúa)*

# 13. Gestión de los incidentes de la seguridad de la información

## 13.1 Reporte sobre los eventos y las debilidades de la seguridad de la información

Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada.

Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los activos de la organización.
Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

### *13.1.1 Reporte sobre los eventos de seguridad de la información*

*Control*
Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

*Guía de implementación*
Se debería instaurar un procedimiento formal para el reporte de los eventos de seguridad de la información junto con un procedimiento de escalada y respuesta ante el incidente que establezca la acción que se ha de tomar al recibir el reporte sobre un evento de seguridad de la información. Se debería establecer un punto de contacto para el reporte de los eventos de seguridad de la información. Es conveniente garantizar que este punto de contacto se conoce en toda la organización, siempre está disponible y puede suministrar respuesta oportuna y adecuada.

Todos los empelados, contratistas y usuarios de tercera parte deberían tener conciencia de su responsabilidad para reportar todos los eventos de seguridad de la información lo más pronto posible. Deberían conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto. Los procedimientos de reporte deberían incluir los siguientes aspectos:

a) procesos adecuados de retroalimentación para garantizar que aquellos que reportan los eventos de seguridad de la información reciben notificación de los resultados después de que se ha tratado y solucionado el problema;

b) formatos para el reporte de los eventos de seguridad de la información para contener la acción de reporte y ayudar a que la persona que hace el reporte recuerde todas las acciones necesarias en caso de un evento de seguridad de la información;

c) el comportamiento correcto en caso de un evento de seguridad de la información, es decir:

   1) tomar nota inmediatamente sobre los detalles importantes (por ejemplo, tipo de incumplimiento o violación, disfunción que se presenta, mensajes en la pantalla, comportamiento extraño);

   2) no ejecutar ninguna acción propia sino reportarla inmediatamente al punto de contacto;

d) referencia a un proceso disciplinario formal establecido para tratar a los empleados, contratistas o usuarios de tercera parte que cometieron la violación de la seguridad.

En entornos de alto riesgo, se puede suministrar una alarma de coacción[4)] a través de la cual una persona bajo coacción pueda indicar tales problemas. Los procedimientos para responder a las alarmas de coacción deberían reflejar la situación de alto riesgo que indican tales alarmas.

4) Una alarma de coacción es un método para indicar secretamente que tiene lugar una acción "bajo coacción".

*(Continúa)*

*Información adicional*
Los siguientes son ejemplos de eventos e incidentes de seguridad.

a) pérdida del servicio, del equipo o de las prestaciones;
b) mal funcionamiento o sobrecargas del sistema;
c) errores humanos;
d) incumplimientos de las políticas o las directrices;
e) violaciones de las disposiciones de seguridad física;
f) cambios no controlados en el sistema;
g) mal funcionamiento del software o del hardware,
i) violaciones del acceso

Con el debido cuidado de los aspectos de confidencialidad, los incidentes de seguridad de la información se pueden usar en la formación sobre toma de conciencia de los usuarios (véase el numeral 8.2.2) como ejemplos de lo que podría pasar, cómo responder a tales incidentes y cómo evitarlos en el futuro. Para poder tratar adecuadamente los eventos e incidentes de seguridad de la información podría ser necesario recolectar evidencia tan pronto sea posible después del suceso (véase el numeral 13.2.3).

El mal funcionamiento u otro comportamiento anómalo del sistema puede ser un indicador de un ataque de seguridad o una violación real de la seguridad y por lo tanto siempre se debería reportar como evento de seguridad de la información.

Información adicional sobre el reporte de eventos de seguridad de la información y gestión de los incidentes de seguridad de la información se puede encontrar en la norma ISO/IEC TR 18044.

### *13.1.2 Reporte sobre las debilidades en la seguridad*

*Control*
Se debería exigir a todos los empleados, contratistas y usuarios de terceras partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

*Guía de implementación*
Todos los empleados, contratistas y usuarios de terceras partes deberían informar sobre estos asuntos a su director o directamente a su proveedor de servicio, tan pronto sea posible para evitar los incidentes de seguridad de la información. Los mecanismos de reporte deberían ser fáciles, accesibles y disponibles. Se les debería informar a ellos que, en ninguna circunstancia, deberían intentar probar una debilidad sospechada.

*Información adicional*
A todos los empleados, contratistas y usuarios de tercera parte se les debería aconsejar no intentar probar debilidades sospechadas en la seguridad. El ensayo de las debilidades se podría interpretar como un posible uso inadecuado del sistema y también podría causar daño al sistema o servicio de información que origine una responsabilidad legal por la realización individual del ensayo.

## 13.2 Gestión de los incidentes y las mejoras en la seguridad de la información

**Objetivo:** asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, ésta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

*(Continúa)*

### *13.2.1 Responsabilidades y procedimientos*

*Control*
Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

*Guía de implementación*
Además del reporte de los eventos y las debilidades de la seguridad de la información (véase el numeral 13.1), el monitoreo de los sistemas, las alertas y las vulnerabilidades (10.10.2) se debería emplear para detectar los incidentes de la seguridad de la información. Se recomienda tener en cuenta las siguientes directrices para los procedimientos de gestión de los incidentes de seguridad de la información:

a) es conveniente implantar procedimientos para manejar los diferentes tipos de incidentes de seguridad de la información, incluyendo:

   1) fallas en el sistema de información y pérdida del servicio;
   2) códigos maliciosos (véase el numeral 10.4.1);
   3) negación del servicio;
   4) errores producidos por datos del negocio, incompletos o inexactos;
   5) violaciones de la confidencialidad y la integridad;
   6) uso inadecuado de los sistemas de información;

b) además de los planes normales de contingencia (véase el numeral 14.1.3), los procedimientos también deberían comprender (véase el numeral 13.2.2):

   1) el análisis y la identificación de la causa del incidente;
   2) la contención;
   3) la planificación e implementación de la acción correctiva para evitar la recurrencia, si es necesario;
   4) la comunicación con aquellos afectados o implicados con la recuperación después del incidente;
   5) el reporte de la acción a la autoridad apropiada;

c) se deberían recolectar y asegurar las pistas para la auditoría y la evidencia similar (véase el numeral 13.2.3), según sea apropiado para:

   1) el análisis de los problemas internos;
   2) el uso de evidencia forense con respecto a la posible violación del contrato o del requisito reglamentario o en caso de juicios criminales o civiles, por ejemplo, según la legislación sobre uso inadecuado del computador o sobre protección de datos;
   3) la negociación para la compensación proveniente de los proveedores de software y servicios;

d) la acción para la recuperación de las violaciones de la seguridad y la corrección de las fallas del sistema debería estar cuidadosa y formalmente controlada; los procedimientos deberían garantizar que:

   1) únicamente el personal claramente identificado y autorizado tiene acceso a los sistemas y datos activos (véase el numeral 6.2 para el acceso externo);
   2) todas las acciones de emergencia están documentadas en detalle;
   3) la acción de emergencia se reporta a la dirección y se revisa de manera ordenada;
   4) la integridad de los sistemas y controles del negocio se confirma con retraso mínimo.

Los objetivos de la gestión de los incidentes de seguridad de la información se deberían acordar con la dirección y se debería garantizar que los responsables de esta gestión comprenden las prioridades de la organización para el manejo de los incidentes de seguridad de la información.

*Información adicional*
Los incidentes de seguridad de la información podrían trascender las fronteras de la organización y las nacionales. Para responder a tales incidentes existe la necesidad creciente de coordinar la respuesta y compartir la información sobre estos incidentes con las organizaciones externas, según sea apropiado.

*(Continúa)*

***13.2.2 Aprendizaje debido a los incidentes de seguridad de la información***

*Control*
Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

*Guía de implementación*
La información que se obtiene de la evaluación de los incidentes de seguridad de la información se debería utilizar para identificar los incidentes recurrentes o de alto impacto.

*Información adicional*
La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de mejorar o agregar controles para limitar la frecuencia, el daño y el costo de futuras recurrencias, o de considerarlos en el proceso de revisión de la política de seguridad (véase el numeral 5.1.2).

***13.2.3 Recolección de evidencias***

*Control*
Cuando una acción de seguimiento contra una persona u organización después de un incidente de la seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

*Guía de implementación*
Se deberían desarrollar y cumplir procedimientos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la organización.

En general, las reglas para la evidencia comprenden los siguientes aspectos:

a) admisibilidad de la evidencia: si la evidencia se puede utilizar o no en la corte;

b) peso de la evidencia: la calidad y cabalidad de la evidencia.

Para lograr la admisibilidad de la evidencia, la organización debería asegurar que sus sistemas de información cumplen cualquier norma o código de práctica publicado para la producción de evidencia admisible.

El peso de la evidencia suministrada debería cumplir todos los requisitos aplicables.

Para lograr el peso de la evidencia, se debería demostrar la calidad y cabalidad de los controles empleados para proteger correcta y consistentemente la evidencia (es decir, evidencia del control del proceso) en todo el periodo en el cual la evidencia por recuperar se almacenó y procesó, mediante un rastreo sólido de la evidencia. En general, dicho rastreo sólido se puede establecer en las siguientes condiciones:

a) para documentos en papel: el original se guarda con seguridad con un registro de la persona que encontró el documento, el sitio en donde se encontró, la fecha en la cual se encontró y el testigo de tal hallazgo; toda investigación debería garantizar que los originales no han sido alterados;

b) para información en medios de computador: se deberían tomar duplicados o copias (dependiendo de los requisitos que se apliquen) de todos los medios removibles, la información en los discos duros o la memoria para garantizar la disponibilidad; es conveniente conservar el registro de todas las acciones durante el proceso de copiado y dicho proceso debería tener testigos; el medio y el registro originales (si no es posible, al menos un duplicado o copia) se deberían conservar intactos y de forma segura.

Todo el trabajo de peritazgo se debería llevar a cabo únicamente en copias del material de evidencia. Se debería proteger la integridad de todo el material de evidencia. El proceso de copia del material de evidencia debería estar supervisado por personal de confianza y se debería registrar la información sobre cuándo y cómo se realizó dicho proceso, quién ejecutó las actividades de copiado y qué herramientas o programas se utilizaron.

*(Continúa)*

*Información adicional*
Cuando un evento de la seguridad de la información se detecta inicialmente, es posible que no sea obvio si el evento llevará a una acción judicial. Por lo tanto, existe el peligro de destruir intencional o accidentalmente la evidencia necesaria antes de percatarse de la gravedad del incidente. Es aconsejable la participación inicial de un abogado o de la policía en cualquier acción legal contemplada y asesorarse sobre la evidencia requerida.

La evidencia puede trascender las fronteras de la organización y / o las jurisdiccionales. En tales casos, se debería garantizar que la organización tiene derecho a recolectar la información requerida como evidencia. Se deberían tener en cuenta los requisitos de las diferentes jurisdicciones para maximizar las oportunidades de admisión en las jurisdicciones correspondientes.

## 14. Gestión de la continuidad del negocio

### 14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y la recuperación por la pérdida de activos de información en la organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de desastres, fallas de la seguridad, pérdida del servicio y disponibilidad del servicio se deberían someter a un análisis del impacto en el negocio. Se deberían desarrollar e implementar planes de continuidad del negocio para garantizar la restauración oportuna de las operaciones esenciales. La seguridad de la información debería ser una parte integral de todo el proceso de continuidad del negocio y de otros procesos de gestión en la organización.

La gestión de la continuidad del negocio debería incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para los procesos del negocio.

#### *14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio*

*Control*
Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de la seguridad de la información necesarios para la continuidad del negocio de la organización.

*Guía de implementación*
El proceso debería reunir los siguientes elementos clave para la gestión de la continuidad del negocio:

a) comprensión de los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y la determinación de la prioridad de los procesos críticos del negocio (véase el numeral 14.1.2);

b) identificación de todos los activos involucrados en los procesos críticos del negocio (véase el numeral 7.1.1);

*(Continúa)*

c) comprensión del impacto que puedan tener las interrupciones causadas por incidentes de la seguridad de la información (es importante encontrar soluciones para manejar los incidentes que producen impactos menores, así como los incidentes graves que puedan amenazar la viabilidad de la organización), y establecer los objetivos del negocio para los servicios de procesamiento de información;

d) consideración de la adquisición de pólizas de seguros adecuadas que puedan formar parte de todo el proceso de continuidad del negocio y de la gestión de riesgos operativos;

e) identificación y consideración de la implementación de controles preventivos y mitigantes adicionales;

f) identificación de recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requisitos identificados de la seguridad de la información;

g) garantizar la seguridad del personal y la protección de los servicios de procesamiento de información y de la propiedad de la organización;

h) formulación y documentación de los planes de continuidad del negocio que abordan los requisitos de la seguridad de la información acorde con la estrategia acordada de continuidad del negocio (véase el numeral 14.1.3);

i) prueba y actualización regular de los planes y procesos establecidos (véase el numeral 14.1.5);

j) garantizar que la gestión de la continuidad del negocio está incorporada en los procesos y la estructura de la organización; la responsabilidad por el proceso de gestión de la continuidad del negocio se debería asignar en un nivel apropiado en la organización (véase el numeral 6.1.1).

***14.1.2 Continuidad del negocio y evaluación de riesgos***

*Control*
Se deberían identificar los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información.

*Guía de implementación*
Los aspectos de la seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos del negocio de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escala de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los responsables de los recursos y los procesos del negocio. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. Una evaluación debería identificar, cuantificar y priorizar los riesgos frente a los criterios y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridades de recuperación.

Dependiendo de los resultados de una evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez que se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

*(Continúa)*

***14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información***

*Control*
Se deberían desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempo requerido, después de la interrupción o la falla de los procesos críticos para el negocio.

*Guía de implementación*
En el proceso de planificación de la continuidad del negocio se deberían considerar los siguientes aspectos:

a) identificar y acordar todas las responsabilidades y los procedimientos para la continuidad del negocio;

b) identificar la pérdida aceptable de información y servicios;

c) implementar los procedimientos que permitan recuperar y restaurar las operaciones del negocio y la disponibilidad de la información en las escalas de tiempo requeridas; es necesario atender una evaluación de las dependencias internas y externas del negocio y de los contratos establecidos;

d) procedimientos operativos que se han de seguir en espera de la terminación de la recuperación y restauración;

e) documentación de procedimientos y procesos acordados;

f) formación apropiada del personal en los procedimientos y procesos acordados, incluyendo el manejo de las crisis;

g) pruebas y actualización de los planes:

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo la restauración de servicios de comunicación específicos para los clientes en un lapso de tiempo aceptable. Los servicios y recursos que lo facilitan deberían identificarse, incluyendo el personal, los recursos no relacionados con el procesamiento de información, al igual que las disposiciones de respaldo para los servicios de procesamiento de información. Estas disposiciones de respaldo pueden incluir arreglos con terceras partes en forma de acuerdos recíprocos o servicios de suscripción comercial.

Los planes de continuidad del negocio deberían afrontar las vulnerabilidades de la organización y, por lo tanto, pueden contener información sensible que es necesario proteger adecuadamente. Las copias de los planes de la continuidad del negocio se deberían almacenar en un lugar lejano, a suficiente distancia para escapar a cualquier daño por algún desastre en la sede principal. La dirección debería garantizar que las copias de los planes de continuidad del negocio están actualizadas y protegidas con el mismo nivel de la seguridad que se aplica en la sede principal. De igual modo, el otro material necesario para ejecutar los planes de continuidad se debería almacenar en un sitio lejano.

Si se utilizan lugares alternos temporales, el nivel de los controles de la seguridad implementados en estos lugares debería ser equivalente al de la sede principal.

*Información adicional*
Es conveniente observar que los planes y las actividades de la gestión de crisis (véase el numeral 14.1.3.f)) pueden ser diferentes de la gestión de la continuidad del negocio; es decir, se puede presentar una crisis que se pueda adaptar con procedimientos de gestión normales.

***14.1.4 Estructura para la planificación de la continuidad del negocio***

*Control*
Se debería mantener una sola estructura de los planes de continuidad del negocio, para asegurar que todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimiento.

*(Continúa)*

*Guía de implementación*
Cada plan de continuidad del negocio debería describir el enfoque para la continuidad, por ejemplo el enfoque para garantizar la disponibilidad y seguridad de la información o del sistema de información. Igualmente, cada plan debería especificar el plan de escalada y las condiciones para su activación, así como las personas responsables de ejecutar cada componente del plan.

Cuando se identifican nuevos requisitos, todos los procedimientos de emergencia existentes, por ejemplo planes de evacuación o disposiciones de respaldo, se deberían modificar apropiadamente. Los procedimientos se deberían incluir en el programa de gestión de cambios de la organización para garantizar el tratamiento adecuado de los aspectos de la continuidad el negocio.

Cada plan debería tener un responsable específico. Los procedimientos de emergencia, los planes de recursos de emergencia manuales y de reanudación deberían ser responsabilidad de los responsables de los recursos o procesos apropiados del negocio involucrados. Las disposiciones de respaldo para los servicios técnicos alternos, como servicios de procesamiento de información y comunicaciones, usualmente deberían ser responsabilidad de los proveedores del servicio.

Una estructura para la planificación de la continuidad del negocio debería abordar los requisitos de la seguridad de la información identificados y considera los siguientes aspectos:

a) las condiciones para la activación de los planes que describen el proceso a seguir (por ejemplo, la forma de evaluar la situación y quién se va a involucrar) antes de activar cada plan;

b) los procedimientos de emergencia que describen las acciones por realizar tras un incidente que ponga en peligro las operaciones del negocio;

c) los procedimientos de respaldo que describen las acciones por realizar para desplazar las actividades esenciales del negocio o los servicios de soporte a lugares temporales alternos y para devolver la operatividad de los procesos del negocio en los plazos requeridos;

d) los procedimientos operativos temporales por seguir mientras se terminan la recuperación y la restauración;

e) los procedimientos de reanudación que describen las acciones por realizar para que las operaciones del negocio vuelvan a la normalidad;

f) una programación de mantenimiento que especifique cómo y cuándo se realizarán pruebas al plan y el proceso para el mantenimiento del plan;

g) actividades de concienciación, educación y formación diseñadas para comprender los procesos de continuidad del negocio y garantizar que los procesos siguen siendo eficaces;

h) las responsabilidades de las personas, que describan quién es responsable de la ejecución de cada componente del plan. Si se requiere, se deberían nombrar suplentes;

i) los activos y recursos críticos necesarios para ejecutar los procedimientos de emergencia, respaldo y reanudación.

***14.1.5 Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio***

*Control*
Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

*Guía de implementación*
Las pruebas del plan de continuidad del negocio deberían asegurar que todos los miembros del equipo de recuperación y otro personal pertinente son conscientes de los planes y sus responsabilidades para la continuidad del negocio y la seguridad de la información, y conocen su función cuando se ejecuta un plan.

*(Continúa)*

La programación de las pruebas para los planes de continuidad del negocio debería indicar cómo y cuándo se va a probar cada elemento del plan. Cada uno de los elementos se debería probar con frecuencia.

Es conveniente utilizar una variedad de técnicas para garantizar que los planes funcionarán en condiciones reales. Éstas incluirían:

a) la prueba sobre papel de varios escenarios (analizando las disposiciones de recuperación con ayuda de ejemplos de interrupciones);

b) las simulaciones (particularmente para la formación del personal en sus funciones de gestión de crisis / post-incidentes);

c) las pruebas de recuperación técnica (garantizando que los sistemas de información se pueden restaurar eficazmente);

d) Las pruebas de recuperación en un lugar alterno (ejecutando procesos del negocio en paralelo con las operaciones de recuperación fuera de la sede principal);

e) las pruebas de los recursos y servicios del proveedor (asegurando que los servicios y productos proporcionados externamente cumplirán el compromiso contraído);

f) los ensayos completos (probando que la organización, el personal, el equipo, las instalaciones y los procesos pueden hacer frente a las interrupciones).

Cualquier organización puede utilizar estas técnicas. Éstas se deberían aplicar de forma pertinente para el plan específico de recuperación. Se deberían registrar los resultados de las pruebas y, cuando sea necesario, tomar las acciones para mejorar los planes.

Se debería asignar responsabilidad para las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en las disposiciones del negocio que aún no se reflejan en los planes de continuidad del negocio debería ir seguida de una actualización adecuada del plan. Este proceso formal de control de cambios debería garantizar la distribución y el refuerzo de los planes actualizados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios en donde se debería considerar la actualización de los planes de continuidad el negocio incluyen la adquisición de equipos nuevos, la mejora de los sistemas y cambios en:

a) el personal;

b) las direcciones o los números telefónicos;

c) la estrategia del negocio;

d) los lugares, dispositivos y recursos;

e) la legislación;

f) los contratistas, proveedores y clientes principales;

g) los procesos existentes, nuevos o retirados;

h) los riesgos (operativos y financieros).

*(Continúa)*

# 15. Cumplimiento

## 15.1 Cumplimiento de los requisitos legales

Objetivo: evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de la seguridad.

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de la seguridad estatutarios, reglamentarios y contractuales.

Se debería buscar asesoría sobre los requisitos legales específicos de los asesores jurídicos de la organización o de abogados practicantes calificados. Los requisitos legales varían de un país a otro y pueden variar para la información creada en un país y que se transmite a otro (es decir, el flujo de datos trans-fronterizo).

### *15.1.1 Identificación de la legislación aplicable*

*Control*
Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente, documentar y mantener actualizados para cada sistema de información y para la organización

*Guía de implementación*
Los controles específicos y las responsabilidades individuales para cumplir estos requisitos se deberían definir y documentar de forma similar

### *15.1.2 Derechos de propiedad intelectual (DPI)*

*Control*
Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

*Guía de implementación*
Se deberían tomar en consideración las siguientes directrices para proteger todo material que se pueda considerar propiedad intelectual:

a) publicar una política de cumplimiento de los derechos de propiedad intelectual que defina el uso legal del software y de los productos de información;

b) adquirir software únicamente a través de fuentes conocidas y de confianza para garantizar que no se violan los derechos de copia;

c) mantener la concienciación sobre las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias para el personal que los viole;

d) mantener registros apropiados de los activos e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual;

e) mantener prueba y evidencia sobre la propiedad de licencias, discos maestros, manuales, etc.;

f) implementar controles para asegurar que no se excede el número máximo de usuarios permitidos;

g) verificar que únicamente se instalan software autorizado y productos con licencia;

h) suministrar una política para mantener las condiciones de licencia apropiadas;

i) suministrar una política para la disposición o transferencia de software a otros;

j) usar las herramientas de auditoría adecuadas;

*(Continúa)*

k) cumplir los términos y condiciones para el software y la información obtenidos de redes públicas;

l) no duplicar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia;

m) no copiar total ni parcialmente libros, artículos, informes ni otros documentos diferentes a los permitidos por la ley de derechos de copia.

*Información adicional*
Los derechos de propiedad intelectual incluyen derechos de copia de software o de documentos, derechos de diseño, marcas registradas, patentes y licencias de códigos fuente.

Los productos de software patentados usualmente se suministran bajo un acuerdo de licencia que especifica los términos y condiciones de la licencia, por ejemplo, limitar el uso de los productos a máquinas específicas o limitar el copiado a la creación de copias de respaldo únicamente. La situación de DPI del software desarrollado por la organización requiere ser aclarada con el personal.

Los requisitos legales, reglamentarios y contractuales pueden imponer restricciones a la copia de material patentado. En particular pueden exigir que únicamente se utilice el material desarrollado por la organización o que tiene licencia y es suministrado a la organización por quien lo desarrolla. La violación de los derechos de copia puede conducir a acciones legales que pueden implicar procedimientos judiciales.

***15.1.3 Protección de los registros de la organización***

*Control*
Los registros importantes se deberían proteger contra pérdida, destrucción y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

*Guía de implementación*
Los registros se deberían clasificar en tipos de registro, por ejemplo registros de contabilidad, registros de bases de datos, registros de transacciones, registros de auditoría y procedimientos operativos, cada uno con detalles de los periodos de retención y los tipos de medio de almacenamiento como papel, microfichas, medios magnéticos, ópticos, etc. Todo material relacionado con claves criptográficas y programas asociados con archivos encriptados o firmas digitales (véase el numeral 12.3), también se debería almacenar para permitir el descifrado de los registros durante el periodo de tiempo durante el cual se retienen los registros.

Es conveniente tomar en consideración la posibilidad de deterioro de los medios utilizados para almacenar los registros. Los procedimientos de almacenamiento y manipulación se deberían implementar según las recomendaciones del fabricante. Para almacenamiento a largo plazo, se recomienda considerar el uso de papel y microfichas.
Al seleccionar los medios de almacenamiento electrónico, se deberían incluir los procedimientos para garantizar la capacidad de acceso a los datos (facilidad tanto del medio como del formato) durante todo el periodo de retención para salvaguardar contra pérdida debido a cambio en la tecnología futura.

Los sistemas de almacenamiento de datos se deberían seleccionar de forma tal que los datos requeridos se puedan recuperar en el periodo de tiempo y el formato aceptable, dependiendo de los requisitos que se deben cumplir.

El sistema de almacenamiento y manipulación debería garantizar la identificación de los registros y de su periodo de retención tal como se define en los reglamentos o la legislación nacional o regional, si se aplica. Este sistema debería permitir la destrucción adecuada de los registros después de este periodo, si la organización no los necesita.

Para cumplir estos objetivos de salvaguarda de registros, la organización debería seguir los siguientes aspectos:

a) se deberían publicar directrices sobre retención, almacenamiento, manipulación y eliminación de registros e información;

*(Continúa)*

b) es conveniente publicar una programación de retención que identifique los registros y el periodo de tiempo de su retención;

c) se recomienda conservar un inventario de las fuentes de información clave;

d) se deberían implementar los controles apropiados para proteger los registros y la información contra pérdida, destrucción y falsificación.

*Información adicional*
Puede ser necesario retener algunos registros de manera segura para cumplir requisitos estatutarios, reglamentarios o contractuales, así como para dar soporte a las actividades esenciales del negocio. Los ejemplos incluyen los registros que se pueden necesitar como evidencia de que la organización funciona cumpliendo las reglas estatutarias o reglamentarias, para garantizar la defensa adecuada contra potenciales acciones civiles o criminales o para confirmar el estado financiero de la organización con respecto a socios, terceras partes y auditores. El periodo de tiempo y el contenido de los datos para la retención de información pueden ser establecidos por la ley o la reglamentación nacional.
Información adicional sobre la gestión de los registros de la organización se puede encontrar en la norma ISO 15489-1.

***15.1.4 Protección de los datos y privacidad de la información personal***

*Control*
Se debería garantizar la protección de los datos y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica, con las cláusulas del contrato.

*Guía de implementación*
Se debería desarrollar e implementar una política de protección y privacidad de los datos. Esta política se debería comunicar a todas las personas involucradas en el procesamiento de información personal.

El cumplimiento de esta política y de todos los reglamentos y leyes pertinentes a la protección de datos requiere estructura y control adecuados de gestión. Con frecuencia esto se logra mejor nombrando a una persona responsable, como por ejemplo un funcionario para protección de datos, quien debería brindar guía a directores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y los procedimientos específicos que se deberían seguir. La responsabilidad del manejo de la información personal y de la concienciación sobre los principios de protección de datos debería estar acorde con los reglamentos y la legislación correspondientes. Se deberían implementar medidas técnicas y organizacionales apropiadas.

*Información adicional*
Varios países han introducido leyes que imponen controles a la recolección, el procesamiento y la transmisión de datos personales (generalmente se trata de información sobre personas vivas que pueden ser identificadas a partir de tal información).
Dependiendo de la respectiva legislación nacional, estos controles pueden imponer funciones sobre aquellos que recolectan, procesan y distribuyen información personal y pueden restringir la capacidad de transferencia de datos a otros países.

***15.1.5 Prevención del uso inadecuado de los servicios de procesamiento de información***

*Control*
Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósitos no autorizados.

*Guía de implementación*
La dirección debería aprobar el uso de los servicios de procesamiento de información.

Todo uso de estos servicios para propósitos no relacionados con el negocio sin autorización de la dirección (véase el numeral 6.1.4), o para cualquier propósito no autorizado se debería considerar uso inadecuado de los servicios. Si se identifica alguna actividad no autorizada por medio de monitoreo u otros medios, esta actividad debería llamar la atención del director correspondiente para estudiar la acción legal y/o disciplinaria adecuada.

*(Continúa)*

Antes de implementar los procedimientos de monitoreo se debería tener asesoría legal.

Todos los usuarios deberían conocer el alcance preciso de su acceso permitido y del monitoreo implementado para detectar el uso no autorizado. Esto se puede lograr dando a los usuarios autorización escrita, una copia de la cual debería estar firmada por el usuario y la organización debería conservarla. A los empleados de la organización, contratistas y usuarios de terceras partes se les debería advertir que no se permitirá acceso que no esté autorizado.

En el momento del registro de inicio, se debería presentar un mensaje de advertencia que indique que el servicio de procesamiento de información al cual se está ingresando es propiedad de la organización y que no se permite el acceso no autorizado. El usuario debe reconocer y reaccionar apropiadamente al mensaje de la pantalla para continuar con el proceso de registro de inicio (véase el numeral 11.5.1).

*Información adicional*
Los servicios de procesamiento de información de de la organización tienen el fin principal o exclusivo de los propósitos del negocio.

La detección de intrusión, la inspección del contenido y otras herramientas de monitoreo pueden ayudar y evitar el uso inadecuado de los servicios de procesamiento de información.

Muchos países tienen legislaciones que protegen contra el uso inadecuado del computador.

Puede ser un acto criminal usar el computador con propósitos no autorizados.

La legalidad de monitorear la utilización varía de un país a otro y puede exigir que la dirección advierta a los usuarios sobre tal monitoreo y / o obtenga su acuerdo. Cuando el sistema al cual se ingresa se utiliza para acceso público (por ejemplo en un servidor web público) y está sujeto a monitoreo de la seguridad, se debería mostrar un mensaje que así lo indique.

***15.1.6 Reglamentación de los controles criptográficos***

*Control*
Se deberían utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

*Guía de implementación*
Se recomienda tener presentes los siguientes elementos para el cumplimiento con acuerdos, leyes y reglamentos pertinentes:

a) restricción de importaciones y/o exportaciones de hardware y software de computadores para la ejecución de funciones criptográficas;

b) restricción de importaciones y/o exportaciones de hardware y software de computadores diseñados para adicionarles funciones criptográficas;

c) restricciones al uso de encriptación;

d) métodos obligatorios o discrecionales de acceso por parte de las autoridades del país a la información encriptada mediante hardware o software para brindar confidencialidad al contenido.

Se debería buscar asesoría legal para garantizar el cumplimiento con las leyes y los reglamentos nacionales. Antes de desplazar la información encriptada o los controles criptográficos a otros países, se debería tener asesoría legal.

*(Continúa)*

## 15.2 Cumplimiento de las políticas y las normas de la seguridad y cumplimiento técnico

Objetivo: asegurar que los sistemas cumplen con las normas y políticas de la seguridad de la organización.

La seguridad de los sistemas de información se debería revisar a intervalos regulares.

Dichas revisiones se deberían llevar a cabo frente a las políticas de la seguridad apropiadas y se deberían auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y los controles de la seguridad documentados.

### *15.2.1 Cumplimiento con las políticas y las normas de la seguridad*

*Control*
Los directores deberían garantizar que todos los procedimientos de la seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las normas de la seguridad.

*Guía de implementación*
Los directores deberían revisar con regularidad en su área de responsabilidad el cumplimiento del procesamiento de información con las políticas de la seguridad adecuadas, las normas y cualquier otro requisito de la seguridad.

Si se halla algún incumplimiento como resultado de la revisión, los directores deberían:

a) determinar la causa del incumplimiento;

b) evaluar la necesidad de acciones para garantizar que no se presenten incumplimientos;

c) determinar e implementar la acción correctiva apropiada,

d) revisar la acción correctiva que se ejecutó.

Se deberían registrar los resultados de las revisiones y las acciones correctivas llevadas a cabo por los directores y conservar dichos registros. Los directores deberían informar de los resultados a las personas que realizan revisiones independientes (véase el numeral 6.1.8), cuando la revisión independiente tiene lugar en el área de su responsabilidad.

*Información adicional*
En el numeral 10.10 se discute el monitoreo operativo del sistema.

### *15.2.2 Verificación del cumplimiento técnico*

*Control*
Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.

*Guía de implementación*
La verificación del cumplimiento técnico se debería realizar bien sea manualmente (con soporte de las herramientas de software apropiadas, si es necesario) por un ingeniero de sistemas con experiencia y/o con la ayuda de herramientas automáticas que generan un informe técnico para la interpretación posterior por parte del especialista técnico.

Si se utilizan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tener cuidado puesto que dichas actividades pueden poner en peligro la seguridad del sistema. Tales pruebas se deberían planificar, documentar y ser repetibles.

La verificación del cumplimiento técnico únicamente la deberían realizar personas autorizadas y competentes o bajo supervisión de dichas personas.

*(Continúa)*

*Información adicional*
La verificación del cumplimiento técnico involucra el examen de los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Este tipo de verificación del cumplimiento requiere experiencia técnica especializada.

La verificación del cumplimiento también comprende, por ejemplo pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados para este propósito. Ello puede ser útil para detectar vulnerabilidades en el sistema y verificar qué tan efectivos son los controles evitando el acceso no autorizado debido a estas vulnerabilidades.

Las pruebas de penetración y las evaluaciones de vulnerabilidad proveen una visión instantánea de un sistema en un estado específico en un momento específico. Esta instantánea se limita a aquellas porciones del sistema que se someten a prueba real durante el (los) intento (s) de penetración. Las pruebas de penetración y las evaluaciones de vulnerabilidad no substituyen a una evaluación de riesgos.

## 15.3 Consideraciones de la auditoría de los sistemas de información

Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.

Deberían existir controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorías de los sistemas de información.

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

### *15.3.1 Controles de auditoría de los sistemas de información*

*Control*
Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

*Guía de implementación*
Se deberían tener presente las siguientes directrices:

a) los requisitos de auditoría se deberían acordar con la dirección correspondiente;

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

c) las verificaciones se deberían limitar al acceso de sólo lectura del software y los datos;

d) el acceso diferente al de sólo lectura únicamente se debería permitir para copias aisladas de archivos del sistema que se puedan borrar al terminar la auditoría, o se debería dar protección adecuada, si existe la obligación de conservar dichos archivos según los requisitos de documentación de la auditoría;

e) los recursos para llevar a cabo las verificaciones se deberían identificar explícitamente y estar disponibles;

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

g) todo acceso se debería monitorear y registrar para crear un rastreo para referencia; el uso de rastreos de referencia de tiempo se debería considerar para datos o sistemas críticos;

h) se recomienda documentar todos los procedimientos, requisitos y responsabilidades;

i) la persona que realiza la auditoría debería ser independiente de las actividades auditadas.

*(Continúa)*

***15.3.2 Protección de las herramientas de auditoría de los sistemas de información***

*Control*
Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

*Guía de implementación*
Las herramientas de auditoría de los sistemas de información, por ejemplo, software o archivos de datos, se deberían separar de los sistemas operativos y de desarrollo y no mantenerse en librerías de cinta, salvo que se les proporcione un nivel adecuado de protección adicional.

*(Continúa)*

## Bibliografía

ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary

ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework

ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General

ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

ISO 10007:2003 Quality management systems – Guidelines for configuration management

ISO/IEC 12207:1995 Information technology – Software life cycle processes

ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002 OECD Guidelines for Cryptography Policy, 1997

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access

ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management

ISO/IEC 27002:2005 *Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información*

## APÉNDICE Z

### Z.1 DOCUMENTOS NORMATIVOS A CONSULTAR

| | |
|---|---|
| ISO/IEC Guide 2 | *Standardization and related activities – General vocabulary* |
| ISO/IEC Guide 73 | *Risk management – Vocabulary – Guidelines for use in standards* |
| ISO/IEC 13335-1 | *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management* |
| ISO/IEC TR 13335-3 | *Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security* |
| ISO/IEC 13888-1 | *Information technology – Security techniques – Non-repudiation – Part 1: General* |
| ISO/IEC 11770-1 | *Information technology – Security techniques – Key management – Part 1: Framework* |
| ISO/IEC 9796-2 | *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms* |
| ISO/IEC 9796-3 | *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms* |
| ISO/IEC 14888-1 | *Information technology – Security techniques – Digital signatures with appendix – Part 1: General* |
| ISO/IEC 15408-1 | *Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model* |
| ISO/IEC 14516 | *Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services* |
| ISO 15489-1 | *Information and documentation – Records management – Part 1: General* |
| ISO 10007 | *Quality management systems – Guidelines for configuration management* |
| ISO/IEC 12207 | *Information technology – Software life cycle processes* |
| ISO 19011 | *Guidelines for quality and /or environmental management systems auditing OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002. OECD Guidelines for Cryptography Policy, 1997* |
| IEEE P1363-2000 | *Standard Specifications for Public-Key Cryptography* |
| ISO/IEC 18028-4 | *Information technology – Security techniques – IT Network security – Part 4: Securing remote access* |
| ISO/IEC TR 18044 | *Information technology – Security techniques – Information security incident management* |
| ISO/IEC 27002 | *Tecnología de la información. Técnicas de la seguridad. Código de práctica para la gestión de la seguridad de la información* |

### Z.2 BASES DE ESTUDIO

Esta norma es una adopción de la ISO/IEC 27002:2005(E). *Information technology – Security techniques – Code of practice for information security management.* International Organization for Standardization ISO. Geneve, 2005.

## INFORMACIÓN COMPLEMENTARIA

| **Documento:** | **TÍTULO: TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE LA SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | **Código:** |
|---|---|---|
| NTE INEN-ISO 27002 | | **TI 01.01-601** |

| ORIGINAL: | REVISIÓN: |
|---|---|
| Fecha de iniciación del estudio: | Fecha de aprobación anterior del Directorio<br>Oficialización con el Carácter de<br>por Resolución No. de<br>publicado en el Registro Oficial No. de<br><br>Fecha de iniciación del estudio: |

Fechas de consulta pública: de a

Comité Interno del INEN:
Fecha de iniciación: 2008-12-30 Fecha de aprobación: 2008-12-31
Integrantes del Comité Interno:

| **NOMBRES:** | **INSTITUCIÓN REPRESENTADA:** |
|---|---|
| Dr. Ramiro Gallegos (Presidente) | DIRECTOR DEL ÁREA TÉCNICA DE SERVICIOS TECNOLÓGICOS |
| Ing. Fausto Lara | ÁREA TÉCNICA DE NORMALIZACIÓN |
| Ing. Elizabeth Guerra | ÁREA TÉCNICA DE CERTIFICACIÓN |
| Sr. Edgar Valenzuela (Secretario Técnico) | ÁREA DE INFORMÁTICA |

Otros trámites:

El Directorio del INEN aprobó este proyecto de norma en sesión de 2009-03-27

Oficializada como: Voluntaria Por Resolución No. 032-2009 de 2009-05-04
Registro Oficial No. 596 de 2009-05-22

**Instituto Ecuatoriano de Normalización, INEN - Baquerizo Moreno E8-29 y Av. 6 de Diciembre**
**Casilla 17-01-3999 - Telfs: (593 2)2 501885 al 2 501891 - Fax: (593 2) 2 567815**
**Dirección General: E-Mail:direccion@inen.gov.ec**
**Área Técnica de Normalización: E-Mail:normalizacion@inen.gov.ec**
**Área Técnica de Certificación: E-Mail:certificacion@inen.gov.ec**
**Área Técnica de Verificación: E-Mail:verificacion@inen.gov.ec**
**Área Técnica de Servicios Tecnológicos: E-Mail:inencati@inen.gov.ec**
**Regional Guayas: E-Mail:inenguayas@inen.gov.ec**
**Regional Azuay: E-Mail:inencuenca@inen.gov.ec**
**Regional Chimborazo: E-Mail:inenriobamba@inen.gov.ec**
**URL:www.inen.gov.ec**