# NORMA CHILENA NCh-ISO 27001

Segunda edición
2013.10.25

## Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos

*Information technology - Security techniques - Information security management systems - Requirements*

Número de referencia
NCh-ISO 27001:2013

## DOCUMENTO PROTEGIDO POR COPYRIGHT



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

## Contenido

Página

# Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos

## Preámbulo

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

Esta norma se estudió por el Comité Técnico *Conjunto de caracteres y codificación*, y define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de la organización.

Esta norma es idéntica a la versión en inglés de la Norma ISO/IEC 27001:2013 *Information technology - Security techniques - Information security management systems - Requirements.*

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

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

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

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

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

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

# Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos

## 0 Introducción

### 0.1 General

Esta norma ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información. La adopción del sistema de gestión de la seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de la seguridad de la información de la organización está influenciada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y la estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de la seguridad de la información conserva la confidencialidad, integridad y disponibilidad de la información al aplicar un proceso de gestión de riesgo y le entrega confianza a las partes interesadas cuyos riesgos son gestionados de manera adecuada.

Es importante que el sistema de gestión de seguridad de la información sea parte de y este integrado a los procesos de la organización y a la estructura de gestión general y que la seguridad de la información sea considerada en el diseño de procesos, sistemas de información y controles. Se espera que la implementación del sistema de gestión de la seguridad de la información sea escalada según las necesidades de la organización.

Esta norma puede ser usada por las partes internas y externas para evaluar la capacidad de la organización para cumplir con los propios requerimientos de seguridad de la información de la organización.

El orden en que se presentan los requerimientos en esta norma no refleja su importancia ni implica el orden en que serán implementados. La lista de elementos está enumerada solo como referencia.

ISO/IEC 27000 describe las generalidades y el vocabulario de los sistemas de la gestión de la seguridad de la información, relacionando la familia del sistema de gestión de la seguridad de la información de las normas (incluidos ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), con los términos y definiciones relacionados.

### 0.2 Compatibilidad con otras normas de sistema de gestión

Esta norma aplica la estructura de alto nivel, los títulos de sub-cláusula idénticos, el texto idéntico, los términos en común y las definiciones clave definidas en Anexo SL de las Directivas de ISO/IEC, Parte 1, Suplemento ISO Consolidado y por lo tanto, mantiene la compatibilidad con otras normas del sistema de gestión que Anexo SL adoptó.

Este enfoque común definido en Anexo SL será útil para aquellas organizaciones que opten por trabajar con un solo sistema de gestión que cumpla con los requisitos de dos o más normas del sistema de gestión.

## 1 Alcance y campo de aplicación

Esta norma define los requerimientos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, dentro del contexto de la organización. Esta norma incluye además los requisitos para la evaluación y tratamiento de los riesgos de la seguridad de la información que se adapta a las necesidades de la organización. Los requisitos definidos en esta norma son genéricos y tienen por objetivo ser aplicables a todas las organizaciones, sin importar el tipo, tamaño o naturaleza. A excepción de los requisitos especificados en cláusulas 4 a la 10, no es aceptable cuando una organización reclama la conformidad de esta norma.

## 2 Referencias normativas

En este documento se hace referencia en forma normativa a los siguientes documentos, completos o parte de ellos, los que son indispensables para su aplicación. Para referencias con fecha, sólo aplica la edición citada. Para referencias sin fecha, se aplica la última edición del documento referenciado (incluyendo cualquier enmienda).

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

**NOTA EXPLICATIVA NACIONAL**

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

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

## 3 Términos y definiciones

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

## 4 Contexto de la organización

### 4.1 Comprender la organización y su contexto

La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr e(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información.

NOTA Determinar estos asuntos se refiere a establecer el contexto externo e interno de la organización, considerado en ISO 31000:2009, 5.3.

### 4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información; y

b) los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requerimientos legales y regulatorios, así como obligaciones contractuales.

### 4.3 Determinar el alcance del sistema de gestión de la seguridad de la información

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.

Al determinar este alcance, la organización debe considerar:

a) los asuntos externos e internos tratados en 4.1;

b) los requerimientos tratados en 4.2; y

c) interferencias y dependencias entre las actividades realizadas por la organización y aquellas realizadas por otras organizaciones.

El alcance estará disponible como información documentada.

### 4.4 Sistema de gestión de la seguridad de la información

La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma.

## 5 Liderazgo

### 5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información al:

a) asegurar que los objetivos de la política de seguridad de la información y la seguridad de la información se establezcan y sean compatibles con la dirección estratégica de la organización;

b) asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información a los procesos de la organización;

c) asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información están disponibles;

d) comunicar la importancia de la gestión de seguridad de la información efectiva y del cumplimiento de los requisitos del sistema de gestión de la seguridad de la información;

e) asegurar que el sistema de gestión de la seguridad de la información logre su(s) resultado(s) esperado(s);

f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información;

g) promover la mejora continua; y

h) apoyar otros roles de gestión relevantes para demostrar su liderazgo, según corresponda a sus áreas de responsabilidad.

### 5.2 Política

La alta dirección debe establecer una política de seguridad de la información que:

a) es pertinente al objetivo de la organización;

b) incluya los objetivos de seguridad de la información (consulte 6.2) o que proporcione el marco de trabajo para establecer los objetivos de seguridad de la información;

c) incluye un compromiso para satisfacer los requisitos aplicables, relacionados a la seguridad de la información; y

d) incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información debe:

e) estar disponible como información documentada;

f) ser comunicada dentro de la organización; y

g) estar disponible para las partes interesadas, según corresponda.

### 5.3 Roles organizacionales, responsabilidades y autoridades

La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.

La alta dirección debe asignar la responsabilidad y la autoridad para:

a) asegurar que el sistema de gestión de la seguridad de la información cumple con los requisitos de esta norma; y

b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.

NOTA Además, la alta dirección puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.

## 6 Planificación

### 6.1 Acciones para abordar los riesgos y las oportunidades

#### 6.1.1 General

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar los asuntos tratados en 4.1 y los requisitos tratados en 4.2 y determinar los riesgos y oportunidades que necesitan ser cubiertos para:

a) asegurar que el sistema de gestión de la seguridad de la información pueda lograr su(s) resultado(s) esperado(s);

b) evitar o disminuir efectos no deseados; y

c) lograr una mejora continua.

La organización debe planificar:

d) acciones para abordar estos riesgos y oportunidades; y

e) cómo

1) integrar e implementar las acciones en los procesos del sistema de gestión de la seguridad de la información; y

2) evaluar la eficacia de estas acciones.

**6.1.2 Evaluación de riesgo de la seguridad de la información**

La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información que:

a) establezca y mantenga los criterios de riesgo de la seguridad de la información que incluya:

1) los criterios de aceptación del riesgo; y

2) los criterios para realizar las evaluaciones de riesgo de la seguridad de la información;

b) asegure que las evaluaciones de riesgo de la seguridad de la información, producen resultados consistentes, válidos y comparables, una y otra vez;

c) identifica los riesgos de la seguridad de la información:

1) aplica el proceso de evaluación del riesgo de la seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de la seguridad de la información; y

2) identifica los propietarios del riesgo;

d) analiza los riesgos de la seguridad de la información:

1) evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2 c) 1) se hicieran realidad;

2) evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y

3) determina los niveles de riesgo;

e) evalúa los riesgos de la seguridad de la información:

1) compara los resultados del análisis de riesgo con los criterios de riesgo definidos en 6.1.2 a); y

2) prioriza los riesgos analizados para el tratamiento de riesgo.

La organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información.

 

#### 6.1.3 Tratamiento de riesgo de la seguridad de la información

La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para:

a) seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo;

b) determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida;

NOTA Las organizaciones pueden diseñar controles, según sea necesario, o identificarlos desde cualquier fuente.

c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido;

NOTA 1 Anexo A contiene una completa lista de objetivos de control y controles. Los usuarios de esta norma son dirigidos al Anexo A para asegurar que ningún control necesario se pasó por alto.

NOTA 2 Los objetivos de control se incluyen de manera implícita en los controles escogidos. Los objetivos de control y los controles enumerados en Anexo A no son exhaustivos, por lo que se podrían necesitar objetivos de control y controles adicionales.

d) generar una Declaración de Aplicabilidad que contenga los controles necesarios[consultar 6.1.3 b) y c)], y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;

e) formular un plan de tratamiento del riesgo de seguridad de la información; y

f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual.

La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.

NOTA La evaluación del riesgo de la seguridad de la información y el proceso de tratamiento en esta norma está alineada con los principios y directrices genéricas provistas en ISO 31000.

### 6.2 Objetivos de seguridad de la información y planificación para lograrlos

La organización debe establecer los objetivos de seguridad de la información en niveles y funciones relevantes. Los objetivos de seguridad de la información deben:

a) ser consistentes con la política de seguridad de la información;

b) ser medible (si es posible);

c) tomar en consideración los requisitos de seguridad de la información aplicable y los resultados de la evaluación de riesgo y el tratamiento de riesgo;

d) ser comunicados; y

e) estar actualizados según corresponda.

La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información.

Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

f) qué se hará;

g) qué recursos se necesitarán;

h) quién será responsable;

i) cuándo se terminará; y

j) cómo se evaluarán los resultados.

## 7 Apoyo

### 7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

### 7.2 Competencias

La organización debe:

a) determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño de seguridad de la información;

b) asegurar que estas personas sean competentes basados en una educación, capacitación o experiencia adecuada;

c) cuando corresponda, tomar las acciones para adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas; y

d) retener la información documentada adecuada como evidencia de competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la disposición de capacitar a, la mentoría de o la reasignación de los empleados actuales; o el empleo o contratación de las personas competentes.

### 7.3 Conocimiento

Las personas que trabajen bajo el control de la organización deben estar al tanto de:

a) la política de seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios del desempeño mejorado de la seguridad de la información; y

c) las implicaciones de no cumplir con los requisitos del sistema de gestión de la seguridad de la información.

### 7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas que sean pertinentes al sistema de gestión de seguridad de la información que incluya:

a) qué comunicar;

b) cuándo comunicarlo;

c) con quién comunicarlo;

d) quién debe comunicarlo; y

e) los procesos que se verán afectados por la comunicación.

### 7.5 Información documentada

#### 7.5.1 General

El sistema de gestión de la seguridad de la información debe incluir:

a) información documentada necesaria para esta norma; y

b) información documentada, definida por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.

NOTA La magnitud de la información documentada para un sistema de gestión de la seguridad de la información puede variar de una organización a otra debido a:

1) el tamaño de la organización y su tipo de actividades, procesos, productos y servicios;

2) la complejidad de los procesos y sus interacciones; y

3) la competencia de las personas.

#### 7.5.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente:

a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);

b) formato (por ejemplo, idioma, versión de software, gráficos) y medio (por ejemplo, papel, digital); y

c) revisión y aprobación para conveniencia y suficiencia.

#### 7.5.3 Control de la información documentada

La información documentada necesaria por el sistema de gestión de la seguridad de la información y por la norma debe ser controlada para asegurar que:

a) está disponible y apropiada para su uso, donde y cuando sea necesario; y

b) está debidamente protegida (por ejemplo, de pérdidas de confidencialidad, uso inapropiado o pérdida de integridad).

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y conservación, incluida la conservación de la legibilidad;

e) control de cambios (por ejemplo, control de versión); y

f) retención y disposición.

Información documentada de origen externo, determinada por la organización, de ser necesario, para la planificación y operación del sistema de gestión de la seguridad de la información debe ser identificado como apropiado y controlado.

NOTA El acceso implica una decisión con respecto al permiso para solo ver la información documentada o el permiso y la autoridad para ver y cambiar la información documentada, etc.

## 8 Operación

### 8.1 Control y planificación operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en 6.1. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información, definidos en 6.2.

La organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario.

La organización se debe asegurar de que los procesos externalizados se determinan y controlan.

### 8.2 Evaluación de riesgo de la seguridad de la información

La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos, considerando los criterios establecidos en 6.1.2 a).

La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.

### 8.3 Tratamiento de riesgo de la seguridad de la información

La organización debe implementar el plan de tratamiento del riesgo de la seguridad de la información.

La organización debe conservar la información documentada de los resultados del tratamiento del riesgo de la seguridad de la información.

# 9 Evaluación de desempeño

## 9.1 Monitoreo, medición, análisis y evaluación

La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de la seguridad de la información.

La organización debe determinar:

a) qué se necesita monitorear y medir, incluidos los controles y procesos de la seguridad de la información;

b) los métodos para monitorear, medir, analizar y evaluar, según corresponda, para asegurar resultados válidos;

NOTA Los métodos seleccionados deberían generar resultados comparables y reproducibles para que sean considerados válidos.

c) cuándo se deben llevar a cabo el monitoreo y la medición;

d) quién debe monitorear y medir;

e) cuándo se deben analizar y evaluar los resultados del monitoreo y la medición; y

f) quién debe analizar y evaluar estos resultados.

La organización debe conservar la información documentada correspondiente, como evidencia de los resultados del monitoreo y medición.

## 9.2 Auditoría interna

La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información:

a) cumple con:

   1) los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y

   2) los requisitos de esta norma;

b) está debidamente implementada y mantenida. La organización debe:

c) planificar, establecer, implementar y mantener programa(s) de auditoría, incluida la frecuencia, métodos, responsabilidades, requisitos de planificación e informes. El (los) programa(s) de auditoría debe(n) considerar la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;

d) definir los criterios de auditoría y el alcance para cada auditoría;

e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;

f) asegurar que los resultados de las auditorías son informados a la dirección pertinente; y

g) conservar la información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.

### 9.3 Revisión de gestión

La alta dirección debe revisar el sistema de gestión de la seguridad de la información en los plazos planificados para asegurar su conveniencia, suficiencia y efectividad continua.

La revisión de la dirección debe considerar:

a) el estado de las acciones, a partir de las revisiones de gestión anteriores;

b) los cambios en los asuntos externos e internos que son pertinentes al sistema de gestión de la seguridad de la información;

c) los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en:

   1) no conformidades y acciones correctivas;

   2) resultados del monitoreo y mediciones;

   3) resultados de auditoría; y

   4) cumplimiento de los objetivos de seguridad de la información;

d) comentarios de las partes interesadas;

e) resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo; y

f) las oportunidades para la mejora continua.

Los resultados de la revisión de dirección deben incluir las decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambios al sistema de gestión de la seguridad de la información.

La organización debe conservar la información documentada como evidencia de los resultados de las revisiones de gestión.

## 10 Mejora

### 10.1 No conformidades y acciones correctivas

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar frente a la no conformidad y si corresponde:

   1) tomar acciones para controlarlo y corregirlo; y

   2) encargarse de las consecuencias;

b) evaluar la necesidad de acción para eliminar las causas de no conformidad, y que así esto no vuelva a ocurrir o que ocurra en otro lugar, al:

   1) revisar la no conformidad;

   2) determinar las causas de las no conformidades; y

   3) determinar si existe una no conformidad similar o podría ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva implementada; y

e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.

Las acciones correctivas deben ser pertinentes a los efectos de las no conformidades halladas.

La organización debe conservar la información documentada como evidencia de:

f) la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y

g) los resultados de cualquier acción correctiva.

### 10.2 Mejora continua

La organización debe mejorar de manera continua la conveniencia, suficiencia y efectividad del sistema de gestión de la seguridad de la información.

# Anexo A
(normativo)

# Objetivos de control de referencia y controles

Los objetivos de control y los controles enumerados en Tabla A.1 se obtuvieron directamente y están alineados con aquellos enumerados en ISO/IEC 27002:2013, cláusulas 5 a 18 y deben ser utilizados con cláusula 6.1.3.

**Tabla A.1 - Objetivos de control y controles**

| | | |
|---|---|---|
| A.5 Políticas de seguridad de la información | | |
| A.5.1 Orientación de la dirección para la seguridad de la información | | |
| Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes. | | |
| A.5.1.1 | Políticas para la seguridad de la información | *Control*<br>La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información. |
| A.5.1.2 | Revisión de las políticas de seguridad de la información | *Control*<br>Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continuas. |
| A.6 Organización de la seguridad de la información | | |
| A.6.1 Organización interna | | |
| Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización. | | |
| A.6.1.1 | Roles y responsabilidades de la seguridad de la información | *Control*<br>Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas. |
| A.6.1.2 | Segregación de funciones | *Control*<br>Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización. |
| A.6.1.3 | Contacto con autoridades | *Control*<br>Se deben mantener los contactos apropiados con las autoridades pertinentes. |
| A.6.1.4 | Contacto con grupos especiales de interés | *Control*<br>Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales. |

(continúa)

 

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.6.1.5 | Seguridad de la información en la gestión de proyecto | *Control*<br>Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto. |
| A.6.2 Dispositivos móviles y trabajo remoto | | |
| Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles. | | |
| A.6.2.1 | Política de dispositivos móviles | *Control*<br>Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles. |
| A.6.2.2 | Trabajo remoto | *Control*<br>Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto. |
| A.7 Seguridad ligada a los recursos humanos | | |
| A.7.1 Previo al empleo | | |
| Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados. | | |
| A.7.1.1 | Selección | *Control*<br>Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos. |
| A.7.1.2 | Términos y condiciones de la relación laboral | *Control*<br>Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información. |
| A.7.2 Durante el empleo | | |
| Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información. | | |
| A.7.2.1 | Responsabilidades de la dirección | *Control*<br>La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. |
| A.7.2.2 | Concientización, educación y formación en seguridad de la información | *Control*<br>Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.7.2.3 | Proceso disciplinario | *Control*<br>Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información. |
| A.7.3 Desvinculación y cambio de empleo | | |
| Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo. | | |
| A.7.3.1 | Responsabilidades en la desvinculación o cambio de empleo | *Control*<br>Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral. |
| A.8 Administración de activos | | |
| A.8.1 Responsabilidad por los activos | | |
| Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes. | | |
| A.8.1.1 | Inventario de activos | *Control*<br>Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos. |
| A.8.1.2 | Propiedad de los activos | *Control*<br>Los activos que se mantienen en inventario deben pertenecer a un dueño. |
| A.8.1.3 | Uso aceptable de los activos | *Control*<br>Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información. |
| A.8.1.4 | Devolución de activos | *Control*<br>Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo. |
| A.8.2 Clasificación de la información | | |
| Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización. | | |
| A.8.2.1 | Clasificación de la información | *Control*<br>La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización. |
| A.8.2.2 | Etiquetado de la información | *Control*<br>Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.8.2.3 | Manejo de activos | *Control*<br>Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización. |
| A.8.3 Manejo de los medios | | |
| Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios. | | |
| A.8.3.1 | Gestión de los medios removibles | *Control*<br>Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización. |
| A.8.3.2 | Eliminación de los medios | *Control*<br>Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales |
| A.8.3.3 | Transferencia física de medios | *Control*<br>Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte. |
| A.9 Control de acceso | | |
| A.9.1 Requisitos de negocio para el control de acceso | | |
| Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información. | | |
| A.9.1.1 | Política de control de acceso | *Control*<br>Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información. |
| A.9.1.2 | Accesos a las redes y a los servicios de la red | *Control*<br>Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente. |
| A.9.2 Gestión de acceso del usuario | | |
| Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios. | | |
| A.9.2.1 | Registro y cancelación de registro de usuario | *Control*<br>Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de acceso. |
| A.9.2.2 | Asignación de acceso de usuario | *Control*<br>Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar los derechos de acceso para todos los tipos de usuarios, a todos los sistemas y servicios. |
| A.9.2.3 | Gestión de derechos de acceso privilegiados | *Control*<br>Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.9.2.4 | Gestión de información secreta de autenticación de usuarios | *Control*<br>Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal. |
| A.9.2.5 | Revisión de los derechos de acceso de usuario | *Control*<br>Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica. |
| A.9.2.6 | Eliminación o ajuste de los derechos de acceso | *Control*<br>Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio. |
| A.9.3 Responsabilidades del usuario | | |
| Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación. | | |
| A.9.3.1 | Uso de información de autenticación secreta | *Control*<br>Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta. |
| A.9.4 Control de acceso al sistema y aplicaciones | | |
| Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones. | | |
| A.9.4.1 | Restricción de acceso a la información | *Control*<br>Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso. |
| A.9.4.2 | Procedimientos de inicio de sesión seguro | *Control*<br>Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro. |
| A.9.4.3 | Sistema de gestión de contraseñas | *Control*<br>Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad. |
| A.9.4.4 | Uso de programas utilitarios privilegiados | *Control*<br>Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación. |
| A.9.4.5 | Control de acceso al código fuente de los programas | *Control*<br>Se debe restringir el acceso al código fuente de los programas. |

(continúa)

 

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.10 Criptografía | | |
| A.10.1 Controles criptográficos | | |
| Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información. | | |
| A.10.1.1 | Política sobre el uso de controles criptográficos | *Control*<br>Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. |
| A.10.1.2 | Gestión de claves | *Control*<br>Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil. |
| A.11 Seguridad física y del ambiente | | |
| A.11.1 Áreas seguras | | |
| Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización. | | |
| A.11.1.1 | Perímetro de seguridad física | *Control*<br>Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información. |
| A.11.1.2 | Controles de acceso físico | *Control*<br>Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado. |
| A.11.1.3 | Seguridad de oficinas, salas e instalaciones | *Control*<br>Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones. |
| A.11.1.4 | Protección contra amenazas externas y del ambiente | *Control*<br>Se debe diseñar y aplicar la protección física contra daños por desastre natural, ataque malicioso o accidentes. |
| A.11.1.5 | Trabajo en áreas seguras | *Control*<br>Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras. |
| A.11.1.6 | Áreas de entrega y carga | *Control*<br>Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.11.2 Equipamiento | | |
| Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos así como la interrupción de las actividades de la organización. | | |
| A.11.2.1 | Ubicación y protección del equipamiento | *Control*<br>El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado. |
| A.11.2.2 | Elementos de soporte | *Control*<br>Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte. |
| A.11.2.3 | Seguridad en el cableado | *Control*<br>Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños. |
| A.11.2.4 | Mantenimiento del equipamiento | *Control*<br>El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad. |
| A.11.2.5 | Retiro de activos | *Control*<br>El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización. |
| A.11.2.6 | Seguridad del equipamiento y los activos fuera de las instalaciones | *Control*<br>Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. |
| A.11.2.7 | Seguridad en la reutilización o descarte de equipos | *Control*<br>Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización. |
| A.11.2.8 | Equipo de usuario desatendido | *Control*<br>Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada. |
| A.11.2.9 | Política de escritorio y pantalla limpios | *Control*<br>Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información. |

(continúa)

 

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.12 Seguridad de las operaciones | | |
| A.12.1 Procedimientos operacionales y responsabilidades | | |
| Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información. | | |
| A.12.1.1 | Procedimientos de operación documentados | *Control*<br>Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten. |
| A.12.1.2 | Gestión de cambios | *Control*<br>Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información. |
| A.12.1.3 | Gestión de la capacidad | *Control*<br>Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema. |
| A.12.1.4 | Separación de los ambientes de desarrollo, prueba y operacionales | *Control*<br>Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación. |
| A.12.2 Protección contra código malicioso | | |
| Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso. | | |
| A.12.2.1 | Controles contra código malicioso | *Control*<br>Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios. |
| A.12.3 Respaldo | | |
| Objetivo: Proteger en contra de la pérdida de datos. | | |
| A.12.3.1 | Respaldo de la información | *Control*<br>Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada. |
| A.12.4 Registro y monitoreo | | |
| Objetivo: Registrar eventos y generar evidencia. | | |
| A.12.4.1 | Registro de evento | *Control*<br>Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información. |

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.12.4.2 | Protección de la información de registros | *Control*<br>Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados. |
| A.12.4.3 | Registros del administrador y el operador | *Control*<br>Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad. |
| A.12.4.4 | Sincronización de relojes | *Control*<br>Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia. |
| A.12.5 Control del software de operación | | |
| Objetivo: Asegurar la integridad de los sistemas operacionales. | | |
| A.12.5.1 | Instalación del software en sistemas operacionales | *Control*<br>Se deben implementar los procedimientos para controlar la instalación del software en los sistemas operacionales. |
| A.12.6 Gestión de la vulnerabilidad técnica | | |
| Objetivo: Evitar la explotación de las vulnerabilidades técnicas. | | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas | *Control*<br>Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado. |
| A.12.6.2 | Restricciones sobre la instalación de software | *Control*<br>Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios. |
| A.12.7 Consideraciones de la auditoría de los sistemas de información | | |
| Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales. | | |
| A.12.7.1 | Controles de auditoría de sistemas de información | *Control*<br>Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio. |
| A.13 Seguridad de las comunicaciones | | |
| A.13.1 Gestión de la seguridad de red | | |
| Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. | | |
| A.13.1.1 | Controles de red | *Control*<br>Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones. |

(continúa)

 

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.13.1.2 | Seguridad de los servicios de red | *Control*<br>Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros. |
| A.13.1.3 | Separación en las redes | *Control*<br>Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes. |
| A.13.2 Transferencia de información | | |
| Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa. | | |
| A.13.2.1 | Políticas y procedimientos de transferencia de información | *Control*<br>Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación. |
| A.13.2.2 | Acuerdos sobre transferencia de información | *Control*<br>Los acuerdos deben abarcar la transferencia segura de la información del negocio entre la organización y terceros. |
| A.13.2.3 | Mensajería electrónica | *Control*<br>La información involucrada en la mensajería electrónica debe ser debidamente protegida. |
| A.13.2.4 | Acuerdos de confidencialidad o no divulgación | *Control*<br>Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización. |
| A.14 Adquisición, desarrollo y mantenimiento del sistema | | |
| A.14.1 Requisitos de seguridad de los sistemas de información | | |
| Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicios en las redes públicas. | | |
| A.14.1.1 | Análisis y especificación de requisitos de seguridad de la información | *Control*<br>Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes. |
| A.14.1.2 | Aseguramiento de servicios de aplicación en redes públicas | *Control*<br>La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación y modificación no autorizada. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.14.1.3 | Protección de las transacciones de servicios de aplicación | *Control*<br>La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje. |
| A.14.2 Seguridad en procesos de desarrollo y soporte | | |
| Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información. | | |
| A.14.2.1 | Política de desarrollo seguro | *Control*<br>Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización. |
| A.14.2.2 | Procedimientos de control de cambios del sistema | *Control*<br>Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios. |
| A.14.2.3 | Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación | *Control*<br>Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización. |
| A.14.2.4 | Restricciones en los cambios a los paquetes de software | *Control*<br>Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta. |
| A.14.2.5 | Principios de ingeniería de sistema seguro | *Control*<br>Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información. |
| A.14.2.6 | Entorno de desarrollo seguro | *Control*<br>Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema. |
| A.14.2.7 | Desarrollo tercerizado | *Control*<br>La organización debe supervisar y monitorear la actividad del desarrollo del sistema tercerizado. |
| A.14.2.8 | Prueba de seguridad del sistema | *Control*<br>Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad |
| A.14.2.9 | Prueba de aprobación del sistema | *Control*<br>Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.14.3 Datos de prueba | | |
| Objetivo: Asegurar la protección de los datos usados para prueba. | | |
| A.14.3.1 | Protección de datos de prueba | *Control*<br>Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa. |
| A.15 Relaciones con el proveedor | | |
| A.15.1 Seguridad de la información en las relaciones con el proveedor | | |
| Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores. | | |
| A.15.1.1 | Política de seguridad de la información para las relaciones con el proveedor | *Control*<br>Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización. |
| A.15.1.2 | Abordar la seguridad dentro de los acuerdos del proveedor | *Control*<br>Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización. |
| A.15.1.3 | Cadena de suministro de tecnologías de la información y comunicaciones | *Control*<br>Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro del producto. |
| A.15.2 Gestión de entrega del servicio del proveedor | | |
| Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor. | | |
| A.15.2.1 | Supervisión y revisión de los servicios del proveedor | *Control*<br>Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor. |
| A.15.2.2 | Gestión de cambios a los servicios del proveedor | *Control*<br>Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles, al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos. |
| A.16 Gestión de incidentes de seguridad de la información | | |
| A.16.1 Gestión de incidentes de seguridad de la información y mejoras | | |
| Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades. | | |
| A.16.1.1 | Responsabilidades y procedimientos | *Control*<br>Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.16.1.2 | Informe de eventos de seguridad de la información | *Control*<br>Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados. |
| A.16.1.3 | Informe de las debilidades de seguridad de la información | *Control*<br>Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios, observada o que se sospeche. |
| A.16.1.4 | Evaluación y decisión sobre los eventos de seguridad de la información | *Control*<br>Los eventos de seguridad de la información se deben evaluar y decidir su van a ser clasificados como incidentes de seguridad de la información. |
| A.16.1.5 | Respuesta ante incidentes de seguridad de la información | *Control*<br>Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados. |
| A.16.1.6 | Aprendizaje de los incidentes de seguridad de la información | *Control*<br>Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros. |
| A.16.1.7 | Recolección de evidencia | *Control*<br>La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia. |
| A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio | | |
| A.17.1 Continuidad de la seguridad de la información | | |
| Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad del negocio de la organización. | | |
| A.17.1.1 | Planificación de la continuidad de la seguridad de la información | *Control*<br>La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre. |
| A.17.1.2 | Implementación de la continuidad de la seguridad de la información | *Control*<br>La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (continuación)

| | | |
|---|---|---|
| A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | *Control*<br>La organización debe verificar, de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas. |
| A.17.2 Redundancias | | |
| Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información | | |
| A.17.2.1 | Disponibilidad de las instalaciones de procesamiento de la información | *Control*<br>Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia suficiente para cumplir con los requisitos de disponibilidad. |
| A.18 Cumplimiento | | |
| A.18.1 Cumplimiento con los requisitos legales y contractuales | | |
| Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad. | | |
| A.18.1.1 | Identificación de la legislación vigente y los requisitos contractuales | *Control*<br>Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización. |
| A.18.1.2 | Derechos de propiedad intelectual | *Control*<br>Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados. |
| A.18.1.3 | Protección de los registros | *Control*<br>Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio. |
| A.18.1.4 | Privacidad y protección de la información de identificación personal | *Control*<br>Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda. |
| A.18.1.5 | Regulación de los controles criptográficos | *Control*<br>Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes, y regulaciones pertinentes. |

(continúa)

**Tabla A.1 - Objetivos de control y controles** (conclusión)

| | | |
|---|---|---|
| A.18.2 Revisiones de seguridad de la información | | |
| Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización. | | |
| A.18.2.1 | Revisión independiente de la seguridad de la información | *Control*<br>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 debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos. |
| A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | *Control*<br>Los gerentes deben revisar con regularidad el cumplimiento del procesamiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes. |
| A.18.2.3 | Verificación del cumplimiento técnico | *Control*<br>Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización. |

# Anexo B
(informativo)

# Bibliografía


[1] ISO/IEC 27002:2013 *Information technology - Security Techniques - Code of practice for information security controls.*

[2] ISO/IEC 27003 *Information technology - Security techniques - Information security management system implementation guidance.*

[3] ISO/IEC 27004 *Information technology - Security techniques - Information security management - Measurement.*

[4] ISO/IEC 27005 *Information technology - Security techniques - Information security risk management.*

[5] ISO 31000:2009 *Risk management - Principles and guidelines.*

[6] ISO/IEC Directives, Part 1 *Consolidated ISO Supplement - Procedures specific to ISO, 2012.*


**NOTA EXPLICATIVA NACIONAL**

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

| Norma | Norma nacional | Grado de correspondencia |
|---|---|---|
| ISO/IEC 27002:2013 | NCh-ISO 27002:2013 | La Norma Chilena NCh-ISO 27002:2013 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27002:2013. |
| ISO/IEC 27003 | No hay | - |
| ISO/IEC 27004 | No hay | - |
| ISO/IEC 27005 | NCh-ISO 27005:2009 | La Norma Chilena NCh-ISO 27005:2009 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27005:2008. |
| ISO 31000:2009 | NCh-ISO 31000:2012 | La Norma Chilena NCh-ISO 31000:2012 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO 31000:2009. |

# Anexo C
(informativo)

## Justificación de los cambios editoriales

**Tabla C.1 - Cambios editoriales**

| Cláusula/subcláusula | Cambios editoriales | Justificación |
|---|---|---|
| En toda la norma | Se reemplaza "esta Norma Internacional" por "esta norma". | La norma es de alcance nacional. |
| 1 | Se reemplaza "Alcance" por "Alcance y campo de aplicación". | De acuerdo a estructura de NCh2. |
| 2 y Anexo B | Se agrega Nota Explicativa Nacional. | Para detallar la equivalencia y el grado de correspondencia de las Normas Internacionales con las Normas Chilenas. |

ICS 35.040