NORMA
CHILENA

NCh ISO/IEC 27001

Cuarta edición
2023.08.30

Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

ICS 35.030; 03.100.70

INSTITUTO NACIONAL DE NORMALIZACION

Número de referencia
NCh-ISO/IEC 27001:2023
24 páginas

DOCUMENTO PROTEGIDO POR COPYRIGHT

Instituto Nacional de Normalización - INN

Av. Libertador Bernardo O'Higgins 1449, Santiago Downtown Torre 7, piso 18 • Santiago de Chile

Tel. + 56 2 2445 88 00

Correo Electrónico contacto@inn.cl

Sitio Web www.inn.cl

Publicado en Chile

© ISO/IEC 2022 - Todos los derechos reservados
© INN 2023 - Para la adopción nacional

Contenido

Página

Anexos

Tablas

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 a través del Comité Técnico CL013 *Tecnologías de la información*, para definir los requisitos 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 una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*, y ha sido elaborada por el Instituto Nacional de Normalización.

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

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

El Anexo A forma parte de la norma.

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

Esta norma reemplaza a la norma NCh-ISO/IEC 27001:2020 *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos*, y la deja no vigente técnicamente.

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 30 de agosto de 2023.

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.

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 influenciado 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 de que los 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 se ajuste 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 sus propios requisitos de seguridad de la información.

El orden en que se presentan los requisitos en esta norma no refleja su importancia ni implica el orden en que serán implementados. Los elementos en la lista están enumerados solo como referencia.

ISO/IEC 27000 describe la visión general y el vocabulario de los sistemas de gestión de la seguridad de la información, haciendo referencia a la familia de normas de sistemas de gestión de la seguridad de la información (incluidas 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 subcláusula idénticos, el texto idéntico, términos comunes y las definiciones clave definidas en el 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 han adoptado el Anexo SL.

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 de sistemas de gestión.

Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos

1 Alcance y campo de aplicación

Esta norma define los requisitos 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. No se acepta excluir cualquiera de los requisitos especificados entre las cláusulas 4 a la 10, cuando una organización declara la conformidad con esta norma.

2 Referencias normativas

Los documentos siguientes son indispensables para la aplicación de esta norma. Para referencias con fecha, sólo se 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 las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 27000	NCh-ISO IEC 27000:2018	La Norma Chilena NCh-ISO IEC 27000:2018 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27000:2018.

3 Términos y definiciones

Para los propósitos de esta norma, se aplican los términos y definiciones dados en ISO/IEC 27000.

ISO e IEC mantienen bases terminológicas que se pueden utilizar para normalización en las siguientes direcciones:

— Plataforma en línea de ISO: disponible en https://www.iso.org/obp

— IEC Electropedia: disponible en https://www.electropedia.org

4 Contexto de la organización

4.1 Comprender la organización y su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su objetivo y que afectan su capacidad para lograr el(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 31000:2018, 5.4.1[5]

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;

b) los requisitos pertinentes de estas partes interesadas.

c) cuál de estos requisitos se abordará a través del sistema de gestión de seguridad de la información.

NOTA Los requisitos de las partes interesadas pueden incluir requisitos legales y regulatorios, y 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) las cuestiones externas e internas referidas en 4.1;

b) los requisitos referidos en 4.2;

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

El alcance debe estar 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, incluyendo los procesos necesarios y sus interacciones, según los requisitos 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:

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

b) asegurándose de la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;

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

d) comunicando la importancia de una gestión de seguridad de la información eficaz y conforme con los requisitos del sistema de gestión de la seguridad de la información;

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

f) dirigiendo y apoyando a las personas para contribuir a la eficacia del sistema de gestión de la seguridad de la información;

g) promoviendo la mejora continua; y

h) apoyando a otros roles de pertinentes de la dirección, para demostrar su liderazgo, en la forma en la que aplique a sus áreas de responsabilidad.

NOTA La referencia a “negocios” en esta norma se puede interpretar en sentido amplio para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

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

a) sea adecuada al propósito de la organización;

b) incluya los objetivos de seguridad de la información (véase 6.2) o que proporcione un marco de referencia para establecer los objetivos de seguridad de la información;

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

d) incluya un compromiso de 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;

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 se asignen y se comuniquen dentro de la organización.

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

a) asegurarse que el sistema de gestión de la seguridad de la información es conforme con los requisitos de esta norma;

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

NOTA La alta dirección puede también 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 Generalidades

Al planificar el sistema de gestión de la seguridad de la información, la organización debe considerar las cuestiones referidas en 4.1 y los requisitos referidos en 4.2 y determinar los riesgos y oportunidades que necesitan ser abordados para:

a) asegurar que el sistema de gestión de la seguridad de la información pueda lograr sus resultado previstos;

b) prevenir o reducir los efectos no deseados;

c) lograr la mejora continua.

La organización debe planificar:

d) las acciones para abordar estos riesgos y oportunidades; y

e) la manera de:

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 de riesgo; y

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

b) asegure que evaluaciones de riesgo de la seguridad de la información sucesiva, producen resultados consistentes, válidos y comparables;

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 confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de la seguridad de la información; y

2) identifica los dueños 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 llegan a materializar;

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) valora 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 riesgos de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgos;

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

NOTA 1 Las organizaciones pueden diseñar controles, según sea necesario, o identificarlos desde cualquier fuente.

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

NOTA 2 El Anexo A contiene una lista de posibles controles de seguridad de la información. Los usuarios de esta norma son dirigidos al Anexo A para asegurar que ningún control necesario de seguridad de la información se pase por alto.

NOTA 3 Los controles de seguridad de la información enumerados en Anexo A no son exhaustivos y se pueden incluir controles de seguridad de la información adicionales si es necesario.

d) elaborar una Declaración de Aplicabilidad que contenga:

— los controles necesarios [ver 6.1.3 b) y c)];

— la justificación de las inclusiones;

— si los controles necesarios están implementado o no; y

— la justificación para excluir cualquiera de los controles de Anexo A;

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

f) obtener la aprobación del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de seguridad de la información, por parte del dueño del riesgo.

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

NOTA 4 La evaluación del riesgo de la seguridad de la información y el proceso de tratamiento en esta norma está alineado con los principios y directrices genéricas provistas en ISO 31000.[5]

6.2 Objetivos de seguridad de la información y planificación para lograrlos

La organización debe establecer los objetivos de seguridad de la información en las funciones y niveles pertinentes.

Los objetivos de seguridad de la información deben:

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

b) ser medibles (si es posible);

c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación de riesgo y el tratamiento de riesgo;

d) ser objeto de seguimiento;

e) ser comunicados;

f) actualizarse según corresponda.

g) estar disponible como información documentada.

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:

h) qué se va a hacer;

i) qué recursos se requerirán;

j) quién será responsable;

k) cuándo se finalizará; y

l) cómo se evaluarán los resultados.

6.3 Planificación de los cambios

Cuando la organización determine la necesidad de cambios en el sistema de gestión de seguridad de la información, los cambios se deben llevar a cabo de manera planificada.

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 sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

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

NOTA Las acciones aplicables pueden incluir, por ejemplo, la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación o subcontratación de personas competentes.

7.3 Toma de conciencia

Las personas que trabajen bajo el control de la organización tomen conciencia 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 de una mejora del desempeño de la seguridad de la información; y

c) las implicaciones del incumplimiento de 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 comunicar;

c) a quién comunicar;

d) como comunicarse

7.5 Información documentada

7.5.1 Generalidades

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

a) información documentada necesaria para esta norma; y

b) información documentada que la organización determina como necesaria para la eficacia del sistema de gestión de la seguridad de la información.

NOTA La extensión 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 asegurarse de que lo siguiente sea apropiado:

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, electrónico); y

c) la revisión y aprobación con respecto a la conveniencia y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de la seguridad de la información y por esta norma debe ser controlada para asegurarse de que:

a) esté disponible y sea idónea para su uso, donde y cuando se necesite; y

b) está protegida adecuadamente (por ejemplo, contra pérdida 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 preservación, incluida la preservación de la legibilidad;

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

f) conservación y disposición.

La información documentada de origen externo, que la organización determina como necesaria para la planificación y operación del sistema de gestión de la seguridad de la información, se debe identificar, según sea apropiado y controlar.

NOTA El acceso puede implicar una decisión en relación al permiso, solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

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 cláusula 6, por:

— establecer criterios para los procesos;

— implementar el control de los procesos de acuerdo con los criterios.

La información documentada debe estar disponible en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

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

La organización debe garantizar que los procesos, productos o servicios proporcionados externamente que sean relevantes para el sistema de gestión de la seguridad de la información estén controlados.

8.2 Evaluación de riesgo de la seguridad de la información

La organización debe realizar evaluaciones de riesgo de la seguridad de la información, a 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 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

a) qué necesita seguimiento y medición, incluidos los controles y procesos de la seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos. Los métodos seleccionados deberían generar resultados comparables y reproducibles para que sean considerados válidos.

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

d) quién debe realizar el seguimiento y la medición;

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

f) quién debe analizar y evaluar estos resultados.

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

9.2 Auditoría interna

9.2.1 Generalidades

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

a) cumple con:

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

   2) los requisitos de esta norma;

b) se implementa y se mantiene eficazmente.

9.2.2 Programa de auditoria interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes.

Al establecer el (los) programa(s) de auditoría interna, la organización debe considerar la importancia de los procesos en involucrados y los resultados de auditorías anteriores.

La organización debe:

a) definir los criterios de auditoría y el alcance de cada auditoría;

b) seleccionar los auditores y llevar a cabo las auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;

c) asegurarse de que los resultados de las auditorías se informen a la dirección pertinente.

La información documentada debe estar disponible como evidencia de la implementación del (los) programa(s) de auditoría y los resultados de la auditoría.

9.3 Revisión por la dirección

9.3.1 Generalidades

La alta dirección debe revisar el sistema de gestión de la seguridad de la información a intervalos planificados para asegurar su conveniencia, adecuación y eficacia continua.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir la consideración de:

a) el estado de las acciones de las revisiones por la dirección previas;

b) los cambios en los cuestiones internas y externas que sean pertinentes al sistema de gestión de la seguridad de la información;

c) cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el sistema de gestión de seguridad de la información;

d) la retroalimentación sobre el desempeño de la seguridad de la información, incluidas tendencias en:

   1) las no conformidades y acciones correctivas;

   2) los resultados del seguimiento y medición;

   3) los resultados de las auditorías;

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

e) la retroalimentación de las partes interesadas;

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

g) las oportunidades para la mejora continua.

9.3.3 Salidas de la revisión por la dirección

Las salidas de la revisión por la dirección deben incluir las decisiones relacionadas a las oportunidades de mejora continua y cualquier necesidad de cambios al sistema de gestión de la seguridad de la información.

La información documentada debe estar disponible como evidencia de las salidas de las revisiones por la dirección.

10 Mejora

10.1 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información.

10.2 No conformidades y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

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

   1) tomar acciones para controlarla y corregirla;

   2) hacer frente a las consecuencias;

b) evaluar la necesidad de acción para eliminar las causas de no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, al:

   1) revisar la no conformidad;

   2) determinar las causas de la no conformidad; y

   3) determinar si existen no conformidades similares o que potencialmente puedan ocurrir;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de cualquier acción correctiva tomada; y

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

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

La información documentada debe estar disponible como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción tomada posteriormente,

g) los resultados de cualquier acción correctiva.

Anexo A
(normativo)

Referencia de controles de seguridad de la información

Los controles de seguridad de la información listados en Tabla A.1 se obtuvieron directamente y están alineados con aquellos listados en ISO/IEC 27002:2022[1], cláusulas 5 a 8, y se deben usar en contexto con 6.1.3.

Tabla A.1 – Controles de seguridad de la información

5	**Controles organizacionales**	
5.1	Políticas para la seguridad de la información	*Control* La política de seguridad de la información y las políticas específicas del tema se deben definir, aprobar, comunicar, publicar y dar a conocer por la dirección, al personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.
5.2	Funciones y responsabilidades de seguridad de la información	*Control* Las funciones y responsabilidades de la seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.
5.3	Segregación de funciones	*Control* Se deben segregar los deberes en conflicto y las áreas de responsabilidad en conflicto.
5.4	Responsabilidades de la dirección	*Control* La dirección debe solicitar a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
5.5	Contacto con autoridades	*Control* La organización debe establecer y mantener contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especiales	*Control* La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
5.7	Inteligencia de amenazas	*Control* La información relacionada con las amenazas a la seguridad de la información se debe recopilar y analizar para generar información sobre amenazas.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

5.8	Seguridad de la información en la gestión de proyectos	*Control* Se debe abordar la seguridad de la información en la gestión de proyectos.
5.9	Inventario de información y otros activos asociados	*Control* Se deben desarrollar y mantener un inventario de información y otros activos asociados, incluyendo propietarios.
5.10	Uso aceptable de la información y otros activos asociados	*Control* Se deben identificar, documentar e implementar las reglas para el uso aceptable y procedimientos para el manejo de la información y los activos asociados.
5.11	Retorno de activos	*Control* El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.
5.12	Clasificación de la información	*Control* La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	Etiquetado de la información	*Control* Se deben 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.
5.14	Transferencia de información	*Control* Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
5.15	Control de acceso	*Control* Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar en función de los requisitos comerciales y de seguridad de la información.
5.16	Gestión de identidad	*Control* Se debe gestionar el ciclo de vida completo de las identidades.
5.17	Información de autenticación	*Control* La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

5.18	Derechos de acceso	*Control* Se deben proporcionar, revisar, modificar y eliminar los derechos de acceso a la información y otros activos asociados de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
5.19	Seguridad de la información en la relación con los proveedores	*Control* Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	*Control* Los requisitos pertinentes de seguridad de la información, se deben definir y acordar con cada proveedor en función del tipo de relación con el proveedor.
5.21	Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)	*Control* Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	*Control* La organización debe hacer seguimiento, revisar, evaluar y gestionar cambios periódicamente en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
5.23	Seguridad de la información para el uso de servicios en la nube	*Control* Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	*Control* La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
5.25	Evaluación y decisión sobre los eventos de seguridad de la información	*Control* La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	*Control* Se deben atender los incidentes de seguridad de la información de acuerdo con los procedimientos documentados de control de acceso.
5.27	Aprendizaje de los incidentes de seguridad de la información	*Control* Se debe utilizar el conocimiento obtenido de los incidentes de seguridad de la información para fortalecer y mejorar los controles de seguridad de la información.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

5.28	Recolección de evidencia	*Control* La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionados con eventos de seguridad de la información.
5.29	Seguridad de la información durante la interrupción	*Control* La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.
5.30	Preparación de las TIC para la continuidad del negocio	*Control* La preparación de las TIC se debe planificar, implementar, mantener y probar en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	*Control* Los requisitos legales, estatutarios, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.
5.32	Derechos de propiedad intelectual	*Control* La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	Protección de los registros	*Control* Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización.
5.34	Privacidad y protección de la información de identificación personal (PII)	*Control* La organización debe identificar y cumplir los requisitos relativos a la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
5.35	Revisión independiente de seguridad de la información	*Control* El enfoque de la organización para la gestión de la seguridad de la información y su implementación incluyendo personas, procesos y tecnologías, se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.
5.36	Cumplimiento de políticas, reglas y normas de seguridad de la información	*Control* Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información, las políticas, las reglas y los estándares específicos de cada tema de la organización,
5.37	Procedimientos operativos documentados	*Control* Los procedimientos operativos para las instalaciones de procesamiento de información se deben documentar y poner a disposición del personal que los necesite.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

6	Controles de personas	
6.1	Selección	*Control* Se debe realizar los controles de verificación de antecedentes de manera continua de todos los candidatos para convertirse en personal antes de unirse a la organización de acuerdo con las leyes, regulaciones y normas éticas pertinentes, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
6.2	Términos y condiciones de empleo	*Control* Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.
6.3	Concientización, educación y formación en seguridad de la información	*Control* El personal de la organización y las partes interesadas pertinentes deben recibir la adecuada concientización, educación y formación en seguridad de la información y actualizaciones periódicas en la política de seguridad de la información, las políticas y los procedimientos específicos del tema de la organización, pertinentes para su puesto de trabajo.
6.4	Proceso disciplinario	*Control* Se debe formalizar y comunicar un proceso disciplinario formal para tomar acciones en contra del personal y otras partes interesadas pertinentes que hayan cometido una infracción a la política de seguridad de la información.
6.5	Responsabilidades tras el cese o cambio de empleo	*Control* Se deben definir, aplicar y comunicar las responsabilidades y deberes de seguridad de la información que sigan siendo válidas después del cese o cambio de empleo al personal pertinente y otras partes interesadas.
6.6	Acuerdos de confidencialidad o no divulgación	*Control* Los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la organización para la protección de la información se deben identificar, documentar, revisar regularmente y se debe firmar por el personal y otras partes interesadas pertinentes.
6.7	Trabajo a distancia	*Control* Se deben implementar medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
6.8	Informe de eventos de seguridad de la información	*Control* La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

7	Controles físicos	
7.1	Perímetros de seguridad física	*Control* Los perímetros de seguridad se deben definir y utilizar para proteger las áreas que contienen información y otros activos asociados.
7.2	Acceso físico	*Control* Las áreas seguras se deben proteger por controles de entrada y puntos de acceso apropiados.
7.3	Seguridad de oficinas, salas e instalaciones	*Control* Se debe diseñar e implementar la seguridad física en oficinas, salas e instalaciones.
7.4	Supervisión de seguridad física	*Control* Las instalaciones se deben supervisar continuamente para el acceso físico no autorizado.
7.5	Protección contra amenazas físicas y ambientales.	*Control* Se debe diseñar e implementar la protección contra amenazas físicas y ambientales a la infraestructura, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales.
7.6	Trabajo en áreas seguras	*Control* Se deben diseñar e implementar medidas de seguridad para trabajar en áreas seguras.
7.7	Escritorio despejado y pantalla limpia	*Control* Se deben definir y hacer cumplir apropiadamente las reglas de escritorio despejado de papeles y medios de almacenamiento removibles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
7.8	Ubicación y protección del equipos	*Control* Los equipos se deben ubicar de forma segura y protegida.
7.9	Seguridad de activos fuera de las instalaciones	*Control* Se deben proteger los activos fuera de las instalaciones.
7.10	Medios de almacenamiento	*Control* Se deben administrar los medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	Servicios de apoyo	*Control* Se deben proteger las instalaciones de procesamiento de información contra fallas en el suministro de energía y otras interrupciones causadas por fallas en servicios de apoyo.
7.12	Seguridad de cableado	*Control* Se deben proteger los cables que transportan energía, datos o servicios de información de apoyo contra intercepciones, interferencias o daños.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

7.13	Mantenimiento de equipo	*Control* Se debe mantener correctamente los equipos para asegurar su disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación segura o reutilización de equipos	*Control* Los elementos de los equipos que contengan medios de almacenamiento se deben revisar para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su eliminación o reutilización.
8	Controles tecnológicos	
8.1	Dispositivos terminales del usuario	*Control* Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos terminales del usuario.
8.2	Derechos de acceso privilegiado	*Control* Se debe restringir y administrar la asignación y uso de los derechos de acceso privilegiado.
8.3	Restricción de acceso a la información	*Control* Se debe restringir el acceso a la información y otros activos asociados de acuerdo con la política establecida específica del tema sobre el control de acceso.
8.4	Acceso al código fuente	*Control* Se debe administra apropiadamente el acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software.
8.5	Autenticación segura	*Control* Se deben implementar las tecnologías y procedimientos de autenticación segura en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
8.6	Gestión de capacidad	*Control* Se debe supervisar y ajustar el uso de los recursos de acuerdo con los requisitos de capacidad actuales y esperados.
8.7	Protección contra malware	*Control* Se debe implementar y respaldar la protección contra el malware mediante la concientización adecuada del usuario.
8.8	Gestión de vulnerabilidades técnicas	*Control* Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

8.9	Gestión de configuración	*Control* Se deben establecer, documentar, implementar, hacer seguimiento y revisar las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes.
8.10	Eliminación de información	*Control* La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea requerida.
8.11	Enmascaramiento de datos	*Control* El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
8.12	Prevención fuga de datos	*Control* Se deben aplicar las medidas de prevención de fuga de datos a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Respaldo de información	*Control* Se deben mantener y probar periódicamente los respaldos de seguridad de la información, el software y los sistemas de acuerdo con la política específica de respaldo del tema acordado
8.14	Redundancia de las instalaciones de tratamiento de información	*Control* Se deben implementar las instalaciones de tratamiento de información con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15	Registro	*Control* Se deben producir, almacenar, proteger y analizar registros que examinen actividades, excepciones, fallas y otros eventos pertinentes.
8.16	Actividades de seguimiento	*Control* Se debe hacer seguimiento de las redes, los sistemas y las aplicaciones d por comportamiento anómalo y se debe tomar acciones apropiadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	*Control* Se deben sincronizar los relojes de los sistemas de procesamiento de información utilizados por la organización con las fuentes de tiempo aprobadas.
8.18	Uso de programas de utilidad privilegiados	*Control* Se deben restringir y controlar estrictamente el uso de programas de utilidad que pueden anular el sistema y los controles de aplicación.

(continúa)

Tabla A.1 – Controles de seguridad de la información (continuación)

8.19	Instalación de software en sistemas operativos	*Control* Se deben implementar procedimientos y medidas para administrar de forma segura la instalación de software en los sistemas operativos.
8.20	Seguridad de redes	*Control* Se deben asegurar, administrar y controlar las redes y los dispositivos de redes para proteger la información en los sistemas y aplicaciones.
8.21	Seguridad de servicios de red	*Control* Se deben identificar, implementar y supervisar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Segregación de redes	*Control* Se deben segregar los grupos de servicios de información, usuarios y sistemas de información en las redes de la organización.
8.23	Filtro Web	*Control* Se debe administrar el acceso a sitios web externos para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	*Control* Se deben definir e implementar reglas para el uso eficaz de la criptografía, incluida la administración criptográfica de claves.
8.25	Ciclo de vida de desarrollo seguro	*Control* Se deben establecer y aplicar reglas para el desarrollo seguro de software y sistemas.
8.26	Requisito de Seguridad de las aplicaciones	*Control* Se deben identificar, especificar y aprobar los requisitos de seguridad de la información al desarrollar o adquirir aplicaciones.
8.27	Principios de ingeniería y arquitectura de sistemas seguros	*Control* Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.
8.28	Codificación segura	*Control* Se deben aplicar los principios de codificación segura al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación	*Control* Se deben definir e implementar los procesos de pruebas de seguridad en el ciclo de vida del desarrollo.
8.30	Desarrollo externalizado	*Control* La organización debe dirigir, supervisar y revisar las actividades relacionadas con el desarrollo de sistemas externalizados.

(continúa)

Tabla A.1 – Controles de seguridad de la información (conclusión)

8.31	Separación de entornos de desarrollo, prueba y producción	*Control* Se deben separar y proteger los entornos de desarrollo, prueba y producción.
8.32	Gestión de cambio	*Control* Se deben exponer los cambios en las instalaciones de procesamiento de información y los sistemas de información a procedimientos de gestión de cambios.
8.33	Información de prueba	*Control* Se debe seleccionar, proteger y gestionar apropiadamente la información de pruebas.
8.34	Protección de sistemas de información durante pruebas de auditoría	*Control* Se deben planificar y acordar las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos entre el evaluador y la gerencia correspondiente.

Anexo B
(informativo)

Bibliografía

[1] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection - Information security controls.*

[2] ISO/IEC 27003, *Information technology - Security techniques - Information security management systems - Guidance.*

[3] ISO/IEC 27004, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.*

[4] ISO/IEC 27005, *Information security, cybersecurity and privacy protection - Guidance on managing information security risks.*

[5] ISO 31000:2018, *Risk management - Guidelines*.

NOTA EXPLICATIVA NACIONAL

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

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 27002:2022	NCh-ISO 27002:2022	Idéntica
ISO/IEC 27003	NCh-ISO IEC 27003:2019	La Norma Chilena NCh-ISO 27003:2019 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27003:2017
ISO/IEC 27004	NCh-ISO/IEC TR 27004:2018	La Norma Chilena NCh-ISO/IEC TR 27004:2018 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27004:2016
ISO/IEC 27005	NCh-ISO IEC 27005:2020	La Norma Chilena NCh-ISO 27005:2020 es una adopción idéntica de la versión en inglés de la Norma Internacional ISO/IEC 27005:2018
ISO 31000:2018	NCh-ISO31000:2018	Idéntica

Anexo C
(informativo)

Justificación de los cambios editoriales

Tabla C.1 – Cambios editoriales

Cláusula/subcláusula	Cambios editoriales	Justificación
En toda la norma	Se reemplaza “este documento” por “esta norma”.	De acuerdo con estructura de NCh2.
En toda la norma	Se reemplaza “este documento” por “esta norma”.	La norma es de alcance nacional.
1	Se reemplaza “Alcance” por “Alcance y campo de aplicación”.	De acuerdo con 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.
Anexo B	Se reemplaza “Bibliografía” por “Anexo B (informativo) Bibliografía”.	De acuerdo con estructura de NCh2.