NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27001 2022

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 15046) Lima, Perú

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

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

(EQV. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements)

2022-12-29
3ª Edición

R.D. N° 022-2022-INACAL/DN. Publicada el 2023-01-12 Precio basado en 31 páginas
I.C.S.: 03.100.70; 35.030 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología de la información, seguridad de la información, ciberseguridad, sistemas de gestión, requisitos

INACAL

Calle Las Camelias 817, San Isidro
Lima - Perú
Tel.: +51 1 640-8820
publicaciones@inacal.gob.pe
www.inacal.gob.pe

ÍNDICE

		página
	ÍNDICE	ii
	PRÓLOGO	iv
	PRÓLOGO (ISO/IEC)	vi
	INTRODUCCIÓN	viii
1	Objeto y campo de aplicación	1
2	Referencias normativas	1
3	Términos y definiciones	2
4	Contexto de la organización	2
4.1	Comprender la organización y su contexto	2
4.2	Comprender las necesidades y expectativas de las partes interesadas	2
4.3	Determinar el alcance del sistema de gestión de seguridad de la información	3
4.4	Sistema de gestión de seguridad de la información	3
5	Liderazgo	4
5.1	Liderazgo y compromiso	4
5.2	Política	5
5.3	Roles, responsabilidades y autoridades organizacionales	5
6	Planificación	6
6.1	Acciones para tratar los riesgos y las oportunidades	6
6.2	Objetivos de seguridad de la información y planificación para conseguirlos	9
6.3	Planificación de cambios	10
7	Soporte	10
7.1	Recursos	10
7.2	Competencia	10
7.3	Toma de conciencia	11
7.4	Comunicación	11
7.5	Información documentada	12

8	Operación	13
8.1	Planificación y control operacional	13
8.2	Evaluación de riesgos de seguridad de la información	14
8.3	Tratamiento de riesgos de seguridad de la información	14
9	Evaluación del desempeño	15
9.1	Monitoreo, medición, análisis y evaluación	15
9.2	Auditoría interna	15
9.3	Revisión por la dirección	17
10	Mejoras	18
10.1	Mejora continua	18
10.2	No conformidad y acción correctiva	18
	ANEXO A (NORMATIVA) Controles de seguridad de la información de referencia	20
	BIBLIOGRAFÍA	31

PRÓLOGO

A. RESEÑA HISTÓRICA

A.1 El Instituto Nacional de Calidad - INACAL, a través de la Dirección de Normalización es la autoridad competente que aprueba las Normas Técnicas Peruanas a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en representación del país.

A.2 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de setiembre a noviembre de 2022, utilizando como antecedente a la norma ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

A.3 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, presentó a la Dirección de Normalización -DN-, con fecha 2021-11-10, el PNTP-ISO/IEC 27001:2022 para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2022-11-25. No habiéndose recibido observaciones, fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos**, 3ª Edición, el 12 de enero de 2023.

A.4 Esta tercera edición de la NTP-ISO/IEC 27001 reemplaza a la NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología propia del idioma español y ha sido estructurado de acuerdo a las Guías Peruanas GP 001:2016 y GP 002:2016.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría GS1 Perú

Presidente	Carlos Horna Vallejos
Secretaria	Mary Wong Suehiro
ENTIDAD	**REPRESENTANTE**
Criptografía Legal S. A. C.	Nataly Bravo López Isbert Panez Wuchenauer
GS1 PERÚ	Paola Carhuatanta Montoya
IBM del Perú S. A. C.	Iván Ancco Peña
Indecopi - Gerencia de Planeamiento y Gestión Institucional	César Guerra Camargo
Ministerio de Economía y Finanzas – Dirección General de Asuntos de Economía Internacional, Competencia y Productividad	Luzmila Zegarra Valencia
Oficina de Normalización Previsional – ONP	Jose Valdez Oyola
Secretaría de Gobierno Digital – PCM	Carlos Arias Ramos
SUNAT	Daniel Llanos Panduro
Consultor	Gustavo Vallejo La Torre
Consultor	Marco Bermúdez Torres
Consultor	Ricardo Dioses Villanueva

PRÓLOGO
(ISO/IEC)

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO e IEC, también participan en el trabajo.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en las Directivas ISO/IEC, Parte 1. En particular, se deberían tener en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento fue redactado de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (véase www.iso.org/directives o www.iec.ch/members_experts/refdocs).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO e IEC no deben ser responsables de identificar ninguno o todos los derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (véase www.iso.org/patents) o la lista IEC de declaraciones de patentes recibidas (véase https://patents.iec.ch).

Cualquier nombre comercial utilizado en este documento es información proporcionada para la comodidad de los usuarios y no constituye un respaldo.

Para obtener una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html. En IEC, consulte www.iec.ch/understanding-standards.

Este documento fue preparado por el Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Seguridad de la información, ciberseguridad y protección de la privacidad*.

Esta tercera edición anula y reemplaza la segunda edición (ISO/IEC 27001:2013), que ha sido revisada técnicamente. También incorpora las Corrigendas Técnicas ISO/IEC 27001:2013/COR 1:2014 e ISO/IEC 27001:2013/COR 2:2015.

Los principales cambios son los siguientes:

a) el texto se ha alineado con la estructura armonizada de normas de sistemas de gestión e ISO/IEC 27002:2022.

Cualquier comentario o pregunta sobre este documento debería dirigirse al organismo nacional de normalización del usuario. Se puede encontrar una lista completa de estos organismos en www.iso.org/members.html y www.iec.ch/national-committees.

INTRODUCCIÓN

0.1 Generalidades

Este documento ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de una organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas de que los riesgos se manejan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información sea parte de y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas de la información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca a escala en concordancia con las necesidades de la organización.

Las partes internas y externas pueden utilizar este documento para evaluar la capacidad que tiene la organización de cumplir los requisitos de seguridad de la información de la propia organización.

El orden en el que se presentan los requisitos en este documento no refleja su importancia ni implica el orden en el que van a implementarse. Los elementos de la lista se enumeran únicamente para propósitos de referencia.

ISO/IEC 27000 describe una visión general y el vocabulario de los sistemas de seguridad de la información, haciendo referencia a la familia de normas del sistema de gestión de seguridad de la información (incluyendo ISO/IEC 27003[2], ISO/IEC 27004[3] e ISO/IEC 27005[4], con términos y definiciones relacionadas.

0.2 Compatibilidad con otras normas de sistemas de gestión

Este documento aplica la estructura de alto nivel, títulos de subcapítulos idénticos, texto idéntico, términos comunes, y definiciones básicas proporcionadas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO Consolidado y, por lo tanto, mantiene compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.

Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que elijan operar un sistema de gestión único que satisfaga los requisitos de dos o más normas de sistemas de gestión.

---oooOooo---

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

1 Objeto y campo de aplicación

Esta Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Excluir cualquiera de los requisitos especificados en los capítulos 4 a 10 no es aceptable cuando una organización declara conformidad con esta Norma Técnica Peruana.

2 Referencias normativas

Los siguientes documentos se referencian en esta Norma Técnica Peruana de tal forma que parte o la totalidad de su contenido constituyen requisitos de este documento. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier modificación).

ISO/IEC 27000	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Visión general y vocabulario

3 Términos y definiciones

Para propósitos de esta Norma Técnica Peruana, se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

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

— Electropedia de IEC: disponible en http://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 propósito y que afectan su capacidad de lograr el(los) resultado(s) previstos de su sistema de gestión de seguridad de la información.

NOTA: La determinación de estas cuestiones se refiere al establecimiento del contexto externo e interno de la organización considerado en el subcapítulo 5.4.1 de ISO 31000:2018[5].

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas pertinentes al sistema de gestión de seguridad de la información;

b) los requisitos pertinentes de estas partes interesadas ;

c) cuáles de estos requisitos se abordarán mediante el sistema de gestión de seguridad de la información.

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

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

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

Cuando se determina 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 actividades realizadas por la organización y las que son realizadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de esta Norma Técnica Peruana.

5 Liderazgo

5.1 Liderazgo y compromiso

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

a) asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización;

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

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

d) comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información;

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

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

g) promoviendo la mejora continua; y

h) apoyando a otros roles de gestión pertinentes para demostrar su liderazgo en lo que respecta a sus áreas de responsabilidad.

NOTA: La referencia a "negocios" en este documento puede interpretarse 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) es apropiada al propósito de la organización;

b) incluya objetivos de seguridad de la información (véase 6.2) o proporcione el marco de referencia para fijar los objetivos de seguridad de la información;

c) incluya el compromiso de satisfacer los requisitos aplicables relacionados a la seguridad de la información;

d) incluya el compromiso de mejora continua del sistema de gestión de 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 a las partes interesadas, según corresponda.

5.3 Roles, responsabilidades y autoridades organizacionales

La alta dirección debe asegurar que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información estén asignadas y comunicadas dentro de la organización.

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

a) asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana; y

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

NOTA: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de 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 seguridad de la información, la organización debe considerar las cuestiones referidas en el subcapítulo 4.1 y los requisitos referidos en el subcapítulo 4.2 y determinar los riesgos y oportunidades que necesitan ser abordados para:

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

b) prevenir o reducir los efectos no deseados;

c) lograr la mejora continua.

La organización debe planificar:

d) acciones que aborden estos riesgos y oportunidades; y

e) la forma de:

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

2) evaluar la eficacia de estas acciones.

6.1.2 Evaluación del riesgo de seguridad de la información

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

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

1) los criterios de aceptación del riesgo; y

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

b) asegure que las evaluaciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identifique los riesgos de seguridad de la información

1) aplicando el proceso de evaluación de riesgos de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información; e

2) identificando a los propietarios de los riesgos;

d) analice los riesgos de seguridad de la información:

1) evaluando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse;

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

3) determinando los niveles de riesgo;

e) valore los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a); y

2) priorizando los riesgos analizados para el tratamiento de riesgos.

La organización debe conservar información documentada sobre el proceso de evaluación de riesgos de seguridad de la información.

6.1.3 Tratamiento de riesgos de seguridad de la información

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

a) seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la evaluación de riesgos;

b) determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA 1: Las organizaciones pueden diseñar controles según se requiera, o identificarlos de cualquier fuente.

c) comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario;

NOTA 2: El Anexo A contiene una lista de posibles controles de seguridad de la información. Los usuarios de esta Norma Técnica Peruana son dirigidos al Anexo A para asegurar que no se deje de lado ningún control de seguridad de la información necesario.

NOTA 3: Los controles de seguridad de la información listados en el Anexo A no son exhaustivos y controles de seguridad de la información adicionales pueden ser incluidos de ser necesario.

d) producir una Declaración de Aplicabilidad que contenga:

- los controles necesarios (véase 6.1.3 b) y c));
- la justificación para su inclusión;
- si los controles necesarios están implementados o no; y
- la justificación de excluir controles del Anexo A;

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

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

La organización debe conservar información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

NOTA 4: El proceso de evaluación y tratamiento de riesgos de seguridad de la información en esta Norma Técnica Peruana se alinea con los principios y lineamientos genéricos proporcionados en ISO 31000[5]

6.2 Objetivos de seguridad de la información y planificación para conseguirlos

La organización debe establecer objetivos de seguridad de la información en los niveles y funciones 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) tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la evaluación y tratamiento de riesgos;

d) ser objeto de seguimiento;

e) ser comunicados;

f) actualizarse según corresponda;

g) estar disponible como información documentada.

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

Cuando se planifique cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

h) qué se hará;

i) qué recursos serán requeridos;

j) quién será responsable;

k) cuando se culminará; y

l) cómo los resultados serán evaluados.

6.3 Planificación de cambios

Cuando la organización determina la necesidad de cambios en el sistema de gestión de la seguridad de la información, los cambios deben ser llevados 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 seguridad de la información.

7.2 Competencia

La organización debe:

a) determinar la competencia necesaria de la(s) persona(s) que realizan, bajo su control, un trabajo que afecta al desempeño de la seguridad de la información;

b) asegurar que estas personas son competentes sobre la base de educación, formación, o experiencia adecuados;

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

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

NOTA: Las acciones aplicables pueden incluir, por ejemplo: la provisión de formación, la tutoría o la reasignación de los actuales empleados; o la contratación de personas competentes.

7.3 Toma de conciencia

Las personas que trabajan bajo el control de la organización deben tomar conciencia de:

a) la política de seguridad de información;

b) su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de seguridad de la información; y

c) las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.

7.4 Comunicación

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

a) sobre qué comunicar;

b) cuándo comunicar;

c) con quién comunicarse;

d) cómo comunicarse.

7.5 Información documentada

7.5.1 Generalidades

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

- información documentada requerida por esta Norma Técnica Peruana; e
- información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.

NOTA: La extensión de la información documentada para un sistema de gestión de seguridad de la información puede diferir 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

Cuando se crea y actualiza 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, el lenguaje, versión de software, gráficos) y medios (por ejemplo, papel, electrónico); y

c) revisión y aprobación con respecto a su idoneidada y adecuación.

7.5.3 Control de la información documentada

La información documentada requerida por el sistema de gestión de seguridad de la información y por esta Norma Técnica Peruana se debe controlar para asegurar:

a) que esté disponible y sea adecuada para su uso, donde y cuando sea necesaria; y

b) que esté protegida adecuadamente (por ejemplo, de pérdida de confidencialidad, uso impropio, o pérdida de integridad).

Para el control de la información documentada, la organización debe realizar las siguientes actividades, según sea aplicable:

c) distribución, acceso, recuperación y uso;

d) almacenamiento y preservación, incluyendo la preservación de legibilidad;

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

f) retención y disposición.

La información documentada de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, debe ser identificada según sea apropiado y controlarse.

NOTA: El acceso puede implicar una decisión respecto de la autorización de solamente ver la información documentada, o el permiso y la autoridad de ver y cambiar la información documentada, entre otros.

8 Operación

8.1 Planificación y control operacional

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos, e implementar las acciones determinadas en el capítulo 6, para:

- establecer criterios para los procesos;
- implementar el control de los procesos de acuerdo con los criterios.

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

La organización debe controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurar que los procesos, productos o servicios provistos de forma externa que son pertinentes para el sistema de gestión de seguridad de la información, son controlados.

8.2 Evaluación de riesgos de seguridad de la información

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

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

8.3 Tratamiento de riesgos de seguridad de la información

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

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

9 Evaluación del desempeño

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

a) a qué se necesita hacer seguimiento y ser medido, incluyendo procesos y controles de seguridad de la información;

b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos;

c) cuando se debe realizar el seguimiento y medición;

d) quién debe realizar el seguimiento y medición;

e) cuando los resultados del seguimiento y medición deben ser analizados y evaluados;

f) quién debe analizar y evaluar estos resultados.

La información documentada debe estar disponible como evidencia de los 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 conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

a) está en conformidad con:

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

2) los requisitos de esta Norma Técnica Peruana;

b) está eficazmente implementado y mantenido.

9.2.2 Programa de auditoría interna

La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos de planificación e informes.

Cuando se establezca el (los) programa(s) de auditoría interna, la organización debe tomar en consideración la importancia de los procesos involucrados y los resultados de auditorías previas;

La organización debe:

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

b) seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría;

c) asegurar que los resultados de las auditorías se reporten a los gerentes pertinentes.

Información documentada debe estar disponible como evidencia de la implementación del (de 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 seguridad de la información de la organización a intervalos planificados para asegurar su idoneidad, adecuación y eficacia continua.

9.3.2 Entradas para la revisión por la dirección

La revisión por la dirección debe incluir consideraciones de:

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

b) cambios en las cuestiones externas e internas que son pertinentes al sistema de gestión de 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) retroalimentación sobre el desempeño de seguridad de la información, incluyendo tendencias en:

1) no conformidades y acciones correctivas;

2) resultados del seguimiento y medición;

3) resultados de auditoría;

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

e) retroalimentación de partes interesadas;

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

g) oportunidades para la mejora continua.

9.3.3 Resultados de la revisión por la dirección

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

La información documentada debe estar disponible como evidencia de los resultados de revisiones por parte de la dirección.

10 Mejora

10.1 Mejora continua

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

10.2 No conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según sea aplicable:

   1) tomar acción para controlarla y corregirla;

   2) ocuparse de las consecuencias;

b) evaluar la necesidad de la acción para eliminar las causas de la no conformidad con el fin de que no vuelva a ocurrir u ocurra en otro lugar de las siguientes maneras:

   1) revisando la no conformidad;

   2) determinando las causas de la no conformidad; y

3) determinando si existen no conformidades similares o si podrían ocurrir potencialmente;

c) implementar cualquier acción necesaria;

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

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

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

Información documentada debe estar disponible como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción subsiguiente tomada;

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 la Tabla A.1 son directamente derivados desde y alineados con los listados en ISO/IEC 27002:2022[1], capítulos 5 a 8 y deben ser utilizados en el contexto con el subcapítulo 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 políticas específicas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y conocidas tanto por el personal como por las partes interesadas pertinentes, además revisadas en intervalos planificados y cuando ocurran cambios significativos.
5.2	Roles y responsabilidades en seguridad de la información	**Control** Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.
5.3	Segregación de funciones	**Control** Funciones en conflicto y áreas de responsabilidad en conflicto deben ser segregadas.
5.4	Responsabilidades de la dirección	**Control** La dirección debe requerir 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 procedimientos específicos 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 especiales de interés	**Control** La organización debe establecer y mantener contacto con grupos especiales de interés u otros foros y asociaciones profesionales especializados en seguridad.

5.7	Inteligencia de amenazas	**Control** La información relacionada con las amenazas a la seguridad de la información debe ser recopilada y analizada para producir inteligencia sobre las amenazas.
5.8	Seguridad de la información en la gestión de proyectos	**Control** La seguridad de la información debe estar integrada en la gestión de proyectos.
5.9	Inventario de información y otros activos asociados	**Control** Un inventario de información y otros activos asociados, incluidos los propietarios, debe ser desarrollado y mantenido
5.10	Uso aceptable de la información y otros activos asociados	**Control** Reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados debe ser identificada, documentada e implementada.
5.11	Devolución de activos	**Control** El personal y otras partes interesadas, según sea apropiado, deben devolver todos los activos de la organización en su posesión cuando cambien o terminen su empleo, contrato o acuerdo.
5.12	Clasificación de la información	**Control** La información debe ser clasificada 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 de las partes interesadas pertinentes.
5.13	Etiquetado de la información	**Control** Un conjunto de procedimientos apropiado para el etiquetado de información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la 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 para 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 deben establecerse e implementarse en función de los requisitos del negocio y de seguridad de la información.

5.16	Gestión de identidades	**Control** El ciclo de vida completo de identidades debe ser gestionado.
5.17	Información de autenticación	**Control** La asignación y gestión de la información de autenticación debe ser controlada por un proceso de gestión, incluyendo el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
5.18	Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados deben ser aprovisionados, revisados, modificados y removidos en concordancia con la política específica de la organización y las reglas para el control de acceso.
5.19	Seguridad de la información en las relaciones con los proveedores	**Control** Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios del proveedor.
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	**Control** Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse 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 las tecnologías de la información y comunicación (TIC)	**Control** Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de las TIC.
5.22	Seguimiento, revisión y gestión de cambios en servicios de proveedores	**Control** La organización debe hacer seguimiento, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
5.23	Seguridad de la información en el uso de servicios en la nube	**Control** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse 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 preparar la gestión de los incidentes de seguridad de la información definiendo, estableciendo y comunicando los procesos, las funciones y las responsabilidades de gestión de incidentes de seguridad de la información.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	**Control** La organización debe evaluar los eventos de seguridad de la información y decidir si se categorizan como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	**Control** Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
5.27	Aprendizaje de los incidentes de seguridad de la información	**Control** El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.
5.28	Recolección de evidencia	**Control** La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
5.29	Seguridad de la información durante una interrupción	**Control** La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante una interrupción.
5.30	Preparación de las TIC para la continuidad del negocio	**Control** La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
5.31	Requisitos legales, estatutarios, regulatorios y contractuales	**Control** Los requisitos legales, estatutarios, regulatorios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse 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 registros	**Control** Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
5.34	Privacidad y protección de la información de identificación personal (IIP)	**Control** La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la IIP de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
5.35	Revisión independiente de la seguridad de la información	**Control** El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, procesos y tecnologías, debe revisarse de forma independiente en intervalos planificados o cuando se produzcan cambios significativos.
5.36	Cumplimiento con políticas, reglas y normas de seguridad de la información	**Control** Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas específicas, las reglas y las normas.
5.37	Procedimientos operativos documentados	**Control** Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.
6	**Controles de personal**	
6.1	Selección	**Control** Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accede y a los riesgos percibidos.
6.2	Términos y condiciones del empleo	**Control** Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización con respecto a la seguridad de la información.

6.3	Toma de conciencia, educación y entrenamiento sobre la seguridad de la información	**Control** El personal de la organización y las partes interesadas pertinentes deben recibir una adecuada concientización, educación y capacitación en seguridad de la información, así como actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos, según sea pertinente para su función laboral.
6.4	Proceso disciplinario	**Control** Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.
6.5	Responsabilidades después del cese o cambio de empleo	**Control** Las responsabilidades y obligaciones en materia de seguridad de la información que siguen siendo válidos después del cese o cambio de empleo deben definirse, aplicarse y comunicarse al personal pertinente y otras partes interesadas.
6.6	Acuerdos de confidencialidad o no divulgación	**Control** Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas pertinentes.
6.7	Trabajo remoto	**Control** Se debe implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.
6.8	Reporte 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 bajo sospecha a través de los canales apropiados de manera oportuna.
7	**Controles físicos**	
7.1	Perímetros de seguridad física	**Control** Los perímetros de seguridad deben definirse y utilizarse para proteger las áreas que contienen información y otros activos asociados.

7.2	Ingreso físico	**Control** Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.
7.3	Asegurar oficinas, salas e instalaciones	**Control** Se debe diseñar e implementar la seguridad física para oficinas, salas e instalaciones.
7.4	Supervisión de la seguridad física	**Control** Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.
7.5	Protección contra amenazas físicas y ambientales	**Control** Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
7.6	Trabajo en áreas seguras	**Control** Deben diseñarse e implementarse medidas de seguridad para trabajar en áreas seguras.
7.7	Escritorio y pantalla limpios	**Control** Deben definirse y aplicarse adecuadamente reglas, de papeles y medios de almacenamiento extraíbles y reglas de pantalla limpia en las instalaciones de procesamiento de información.
7.8	Ubicación y protección de los equipos	**Control** Los equipos deben estar ubicados de forma segura y protegidos.
7.9	Seguridad de los activos fuera de las instalaciones	**Control** Los activos fuera del sitio deben protegerse.
7.10	Medios de almacenamiento	**Control** Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación de la organización y los requisitos de manipulación.
7.11	Servicios de suministro de apoyo	**Control** Las instalaciones de procesamiento de información deben protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios de suministro de apoyo.
7.12	Seguridad del cableado	**Control** Los cables que transportan energía, datos o servicios de información de apoyo deben protegerse contra interceptaciones, interferencias o daños.

7.13	Mantenimiento de equipos	**Control** El equipo debe mantenerse correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación segura o reutilización de equipos	**Control** Los elementos del equipo que contienen medios de almacenamiento deben verificarse para asegurar que los datos sensibles y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.
8	**Controles tecnológicos**	
8.1	Dispositivos terminales del usuario	**Control** La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debe protegerse.
8.2	Derechos de acceso privilegiados	**Control** La asignación y el uso de derechos de acceso privilegiado deben restringirse y administrarse.
8.3	Restricción de acceso a la información	**Control** El acceso a la información y otros activos asociados debe restringirse de acuerdo con la política específica establecida sobre control de acceso.
8.4	Acceso al código fuente	**Control** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las librerías de software debe administrarse adecuadamente.
8.5	Autenticación segura	**Control** Se deben implementar tecnologías y procedimientos de autenticación seguros en función de las restricciones de acceso a la información y la política específica sobre el control de acceso.
8.6	Gestión de capacidad	**Control** El uso de recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.
8.7	Protección contra programas maliciosos (*malware*)	**Control** La protección contra programas maliciosos (*malware*) debe implementarse y respaldarse mediante la toma de conciencia 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.
8.9	Gestión de la configuración	**Control** Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
8.10	Eliminación de información	**Control** La información almacenada en sistemas de información, dispositivos o cualquier otro medio de almacenamiento debe eliminarse cuando ya no sea necesaria.
8.11	Enmascaramiento de datos	**Control** El enmascaramiento de datos debe utilizarse de acuerdo con la política específica de la organización sobre control de acceso, otras políticas específicas relacionadas y los requisitos del negocio, teniendo en cuenta la legislación aplicable.
8.12	Prevención de fuga de datos	**Control** Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y otros dispositivos que procesan, almacenan o transmiten información sensible.
8.13	Copia de seguridad de la información	**Control** Las copias de respaldo de la información, el software y los sistemas deben mantenerse y probarse regularmente de acuerdo con la política específica establecida sobre copias de seguridad.
8.14	Redundancia de las instalaciones de procesamiento de información	**Control** Las instalaciones de procesamiento de información deben implementarse con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15	Registro	**Control** Se deben producir, almacenar, proteger y analizar los registros que guarden actividades, excepciones, fallas y otros eventos relevantes.

8.16	Actividades de monitoreo	**Control** Las redes, los sistemas y las aplicaciones deben monitorearse para detectar comportamientos anómalos y tomar acciones para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	**Control** Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse para fuentes de tiempo aprobadas.
8.18	Uso de programas de utilidad privilegiados	**Control** Se debe restringir y controlar estrictamente el uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones.
8.19	Instalación de software en sistemas operativos	**Control** Deben implementarse procedimientos y medidas para gestionar de forma segura la instalación de software en sistemas operativos.
8.20	Seguridad de redes	**Control** Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en sistemas y aplicaciones.
8.21	Seguridad de servicios de red	**Control** Deben identificarse, implementarse y monitorearse los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Segregación de redes	**Control** Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
8.23	Filtrado de la web	**Control** El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	**Control** Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	**Control** Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.
8.26	Requisitos de seguridad de la aplicación	**Control** Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.

8.27	Arquitectura de sistemas seguros y principios de ingeniería	**Control** Los principios de ingeniería de sistemas seguros deben establecerse, documentarse, mantenerse y aplicarse a cualquier actividad de desarrollo de sistema de información.
8.28	Codificación segura	**Control** Los principios de codificación segura deben aplicarse al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación.	**Control** Los procesos de pruebas de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.
8.30	Desarrollo subcontratado	**Control** La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	Separación de los entornos de desarrollo, prueba y producción	**Control** Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
8.32	Gestión de cambios	**Control** Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	Información de las pruebas	**Control** La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.
8.34	Protección de los sistemas de información durante las pruebas de auditoría	**Control** Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

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*