

INTERNACIONAL ESTÁNDAR

**ISO/CEI
27001**

Tercera edición
2022-10

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

*Seguridad de la información, ciberseguridad y protección de la vida
privada — Sistemas de gestión de la seguridad de la información —
Exigencias*



Número de referencia
ISO/CEI 27001:2022(E)

© ISO/CEI 2022



DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR

© ISO/CEI 2022

Reservados todos los derechos. A menos que se especifique lo contrario, o se requiera en el contexto de su implementación, ninguna parte de esta publicación puede ser reproducida o utilizada de ninguna forma o por ningún medio, electrónico o mecánico, incluidas las fotocopias, o la publicación en Internet o en una intranet, sin previo aviso. permiso escrito. El permiso se puede solicitar a ISO en la dirección que se indica a continuación o al organismo miembro de ISO en el país del solicitante.

oficina de derechos de autor ISO
CP 401 • Cap. de Blandonnet 8
CH-1214 Vernier, Ginebra
Teléfono: +41 22 749 01 11 Correo
electrónico: copyright@iso.org
Sitio web: www.iso.org

Publicado en Suiza

Contenido

Página

Prefacio	IV
Introducción	v
1 Alcance	1
2 Referencias normativas	1
3 Términos y definiciones	1
4 Contexto de la organización	1
4.1 Entender la organización y su contexto	1
4.2 Comprender las necesidades y expectativas de las partes interesadas	1
4.3 Determinación del alcance del sistema de gestión de seguridad de la información	2
4.4 Sistema de gestión de seguridad de la información	2
5 Liderazgo	2
5.1 Liderazgo y compromiso	2
5.2 Política	3
5.3 Funciones, responsabilidades y autoridades de la organización	3
6 Planificación	3
6.1 Acciones para abordar riesgos y oportunidades	3
6.1.1 Generalidades	3
6.1.2 Evaluación de riesgos de seguridad de la información	4
6.1.3 Tratamiento de riesgos de seguridad de la información	4
6.2 Objetivos de seguridad de la información y planificación para alcanzarlos	5
7 Apoyo	6
7.1 Recursos	6
7.2 Competencia	6
7.3 Conciencia	6
7.4 Comunicación	6
7.5 Información documentada	6
7.5.1 Generalidades	6
7.5.2 Creación y actualización	7
7.5.3 Control de la información documentada	7
8 Operación	7
8.1 Planificación y control operativo	7
8.2 Evaluación de riesgos de seguridad de la información	8
8.3 Tratamiento de riesgos de seguridad de la información	8
9 Evaluación del desempeño	8
9.1 Seguimiento, medición, análisis y evaluación	8
9.2 Auditoría interna	8
9.2.1 Generalidades	8
9.2.2 Programa de auditoría interna	9
9.3 Revisión por la dirección	9
9.3.1 Generalidades	9
9.3.2 Entradas de la revisión por la dirección	9
9.3.3 Resultados de la revisión por la dirección	9
10 Mejora	10
10.1 Mejora continua	10
10.2 No conformidad y acción correctiva	10
Anexo A(normativo)Referencia de controles de seguridad de la información	11
Bibliografía	19

Prefacio

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 deben 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 (ver www.iso.org/directivas 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 serán 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 (ver www.iso.org/patents) o la lista IEC de declaraciones de patentes recibidas (ver <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 (TBT), consulte www.iso.org/iso/prefacio.html . En la CEI, véase www.iec.ch/understanding-standards .

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

Esta tercera edición cancela y reemplaza la segunda edición (ISO/IEC 27001:2013), que ha sido revisada técnicamente. También incorpora los Corrigenda Técnicos ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015.

Los principales cambios son los siguientes:

— 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 debe dirigirse al organismo nacional de normalización del usuario. Una lista completa de estos organismos se puede encontrar en www.iso.org/members.html y www.iec.ch/comites-nacionales .

Introducción

0.1 generales

Este documento ha sido preparado para proporcionar 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 del 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 la estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de la seguridad de la información forme parte de los procesos y la estructura de gestión general de la organización y se integre con ellos, y que la seguridad de la información se tenga en cuenta en el diseño de los procesos, los sistemas de información y los controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se escale de acuerdo con las necesidades de la organización.

Este documento puede ser utilizado por partes internas y externas para evaluar la capacidad de la organización para cumplir con los requisitos de seguridad de la información de la propia organización.

El orden en que se presentan los requisitos en este documento no refleja su importancia ni implica el orden en que deben implementarse. Los elementos de la lista se enumeran solo con fines de referencia.

ISO/IEC 27000 describe la descripción general y el vocabulario de los sistemas de gestión de seguridad de la información, haciendo referencia a la familia de estándares del sistema de gestión de seguridad de la información (incluido ISO/IEC 27003^[2], ISO/CEI 27004^[3] e ISO/IEC 27005^[4]), con términos y definiciones relacionados.

0.2 Compatibilidad con otros estándares de sistemas de gestión

Este documento aplica la estructura de alto nivel, los títulos de subcláusulas idénticos, el texto idéntico, los términos comunes y las definiciones básicas definidas en el Anexo SL de las Directivas ISO/IEC, Parte 1, Suplemento ISO consolidado y, por lo tanto, mantiene la compatibilidad con otros estándares 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 único sistema de gestión que cumpla con los requisitos de dos o más estándares 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

Este documento 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. Este documento también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en este documento son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Excluyendo cualquiera de los requisitos especificados en [Cláusulas 4 a 10](#) no es aceptable cuando una organización reclama conformidad con este documento.

2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento de referencia (incluidas las modificaciones).

ISO/CEI 27000, *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Visión general y vocabulario*

3 Términos y definiciones

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

ISO e IEC mantienen bases de datos de terminología para su uso en la normalización en las siguientes direcciones:

- Plataforma de navegación ISO Online: disponible en <https://www.iso.org/obp>
- Electropedia IEC: disponible en <https://www.electropedia.org/>

4 Contexto de la organización

4.1 Entender la organización y su contexto

La organización debe determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados de su sistema de gestión de seguridad de la información.

NOTA Determinar estos temas se refiere a establecer el contexto externo e interno de la organización. Considerado en la Cláusula 5.4.1 de la Norma ISO 31000:2018^[5]. —

4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización determinará:

- a) partes interesadas que son relevantes para el sistema de gestión de 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 reglamentarios y requisitos contractuales. obligaciones

4.3 Determinación del alcance del sistema de gestión de 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 a que se refiere el [4.1](#) ;
- b) los requisitos a que se refiere el [4.2](#) ;
- c) interfaces y dependencias entre las actividades realizadas por la organización y aquellas 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 la seguridad de la información, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

5 Liderazgo

5.1 Liderazgo y compromiso

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

- a) garantizar que la política de seguridad de la información y los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización;
- b) garantizar la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;
- c) asegurar que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;
- d) comunicar la importancia de una gestión eficaz de la seguridad de la información y de cumplir con los requisitos del sistema de gestión de la seguridad de la información;
- e) garantizar que el sistema de gestión de la seguridad de la información logre los resultados previstos;
- f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información;
- g) promover la mejora continua; y
- h) apoyar a otros roles gerenciales relevantes para demostrar su liderazgo en lo que se refiere 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 esencial 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 apropiado para el propósito de la organización;
- b) incluye objetivos de seguridad de la información (ver [6.2](#)) o proporciona el marco para establecer objetivos de seguridad de la información;
- c) incluye un compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información;
- d) incluye un compromiso de mejora continua del sistema de gestión de la seguridad de la información.

La política de seguridad de la información deberá:

- e) estar disponible como información documentada;
- f) ser comunicado dentro de la organización;
- g) estar a disposición de los interesados, según corresponda.

5.3 Funciones, responsabilidades y autoridades de la organización

La alta dirección debe asegurarse de que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información se asignen y comuniquen dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) garantizar que el sistema de gestión de la seguridad de la información se ajuste a los requisitos de este documento;
- 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 de la sistema de gestión de la seguridad de la información dentro de la organización.

6 Planificación

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 Generalidades

Al planificar el sistema de gestión de la seguridad de la información, la organización debe tener en cuenta las cuestiones a las que se hace referencia en [4.1](#) y los requisitos a que se refiere el [4.2](#) y determinar los riesgos y oportunidades que deben abordarse para:

- a) garantizar que el sistema de gestión de la seguridad de la información pueda lograr los resultados previstos;
- b) prevenir o reducir los efectos no deseados;
- c) lograr la mejora continua.

La organización debe planificar:

- d) acciones para abordar estos riesgos y oportunidades; y
- e) cómo
 - 1) integrar e implementar las acciones en sus procesos del sistema de gestión de seguridad de la información; y
 - 2) evaluar la efectividad de estas acciones.

6.1.2 Evaluación de riesgos de seguridad de la información

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

a) establece y mantiene criterios de riesgo de seguridad de la información que incluyen:

- 1) los criterios de aceptación del riesgo; y
- 2) criterios para realizar evaluaciones de riesgos de seguridad de la información;

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

c) identifica los riesgos de seguridad de la información:

- 1) aplicar el proceso de evaluación de riesgos de seguridad de la información para identificar los 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; y

- 2) identificar a los propietarios del riesgo;

d) analiza los riesgos de seguridad de la información:

- 1) evaluar las consecuencias potenciales que resultarían si los riesgos identificados en [6.1.2 c\) 1](#)) fueran a materializarse;

- 2) evaluar la probabilidad realista de ocurrencia de los riesgos identificados en [6.1.2 c\) 1](#)); y

- 3) determinar los niveles de riesgo;

e) evalúa los riesgos de seguridad de la información:

- 1) comparar los resultados del análisis de riesgo con los criterios de riesgo establecidos en [6.1.2 a](#)); y

- 2) priorizar 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 apropiadas de tratamiento de riesgos de seguridad de la información, teniendo en cuenta los resultados de la evaluación de riesgos;

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

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

c) comparar los controles determinados en [6.1.3 b](#)) arriba con los de [Anexo A](#) y verificar que no se hayan omitido los controles necesarios;

NOTA 2 [Anexo A](#) contiene una lista de posibles controles de seguridad de la información. Los usuarios de este documento son dirigido a [Anexo A](#) para garantizar que no se pasen por alto los controles necesarios de seguridad de la información.

NOTA 3 Los controles de seguridad de la información enumerados en [Anexo A](#) no son información exhaustiva y adicional se pueden incluir controles de seguridad si es necesario.

d) producir una Declaración de Aplicabilidad que contenga:

- los controles necesarios (ver [6.1.3 b](#)) y c));

- justificación de su inclusión;
 - si se aplican o no los controles necesarios; y
 - la justificación para excluir cualquiera de los [Anexo A](#) control S.
- e) formular un plan de tratamiento de riesgos de seguridad de la información; y
- f) obtener la aprobación 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 este documento se alinea con el principios y directrices genéricas proporcionados en ISO 31000[5].

6.2 Objetivos de seguridad de la información y planificación para alcanzarlos

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

Los objetivos de seguridad de la información deberán:

- a) ser coherente con la política de seguridad de la información;
- b) ser medible (si es factible);
- c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y el tratamiento del riesgo;
- d) ser monitoreado;
- e) ser comunicado;
- f) actualizarse según corresponda;
- g) estar disponible como información documentada.

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

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

- h) lo que se hará;
- i) qué recursos se requerirán;
- j) quién será responsable;
- k) cuándo se completará; y
- l) cómo se evaluarán los resultados.

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 llevarse a cabo de manera planificada.

7 Soporte

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 deberá:

- a) determinar la competencia necesaria de la(s) persona(s) que realiza(n) el trabajo bajo su control que afecta su desempeño en seguridad de la información;
- b) garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas;
- c) en su caso, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad 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 capacitación, tutoría o reasignación de empleados actuales; o la contratación o contratación de personas competentes.

7.3 Conciencia

Las personas que realicen trabajos bajo el control de la organización deberán ser conscientes 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 un mejor desempeño de la seguridad de la información; y
- c) las implicaciones de no cumplir 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 relevantes para el sistema de gestión de la 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 la seguridad de la información de la organización debe incluir:

- a) información documentada requerida por este documento; y

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

NOTA El alcance 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

Al crear y actualizar la información documentada, la organización debe garantizar lo siguiente:

- a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);
- b) formato (p. ej., idioma, versión de software, gráficos) y soporte (p. ej., papel, electrónico); y
- c) revisión y aprobación de la idoneidad 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 este documento se controlará para garantizar:

- a) está disponible y es adecuado para su uso, donde y cuando se necesite; y
- b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

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

- c) distribución, acceso, recuperación y uso;
- d) almacenamiento y conservación, incluida la conservación de la legibilidad;
- e) control de cambios (por ejemplo, control de versiones); 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 identificarse según corresponda y controlarse.

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

8 Operación

8.1 Planificación y control operativo

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en la Cláusula 6, mediante:

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

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

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando medidas 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 riesgos de seguridad de la información

La organización debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan o ocurran cambios significativos, teniendo 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 determinará:

- a) lo que debe monitorearse y medirse, incluidos los procesos y controles de seguridad de la información;
- b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para garantizar la validez de los resultados. Los métodos seleccionados deben producir resultados comparables y reproducibles para que se consideren válidos;
- c) cuándo se realizará el seguimiento y la medición;
- d) quién deberá monitorear y medir;
- e) cuándo se analizarán y evaluarán los resultados del seguimiento y la medición;
- f) quién analizará y evaluará estos resultados.

La información documentada deberá 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 realizar auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información:

- a) se ajusta a
 - 1) los requisitos propios de la organización para su sistema de gestión de seguridad de la información;

- 2) los requisitos de este documento;
- b) se implementa y mantiene de manera efectiva.

9.2.2 Programa de auditoría interna

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

Al establecer los programas de auditoría interna, la organización debe considerar la importancia de los procesos en cuestión y los resultados de auditorías anteriores.

La organización deberá:

- a) definir los criterios de auditoría y el alcance de cada auditoría;
- b) seleccionar auditores y realizar auditorías que garanticen 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 deberá estar disponible como evidencia de la implementación del 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 de la organización a intervalos planificados para garantizar su idoneidad, adecuación y eficacia continuas.

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección incluirá la consideración de:

- a) el estado de las acciones de revisiones de gestión anteriores;
- b) cambios en cuestiones externas e internas que son relevantes para el sistema de gestión de seguridad de la información;
- c) cambios en las necesidades y expectativas de las partes interesadas que sean relevantes para el sistema de gestión de seguridad de la información;
- d) retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias en:
 - 1) no conformidades y acciones correctivas;
 - 2) resultados de monitoreo y medición;
 - 3) resultados de la auditoría;
 - 4) cumplimiento de los objetivos de seguridad de la información;
- e) retroalimentación de las partes interesadas;
- f) resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos;
- g) oportunidades de mejora continua.

9.3.3 Resultados de la revisión por la dirección

Los resultados de la revisión por la dirección incluirán decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión de la seguridad de la información.

La información documentada deberá estar disponible como evidencia de los resultados 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 conformidad y acción correctiva

Cuando ocurre una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según corresponda:

1) tomar acciones para controlarlo y corregirlo;

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acción para eliminar las causas de la no conformidad, a fin de que no se repita u ocurra en otro lugar, mediante:

1) revisar la no conformidad;

2) determinar las causas de la no conformidad; y

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

c) implementar cualquier acción necesaria;

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

e) realizar cambios en el sistema de gestión de seguridad de la información, si es necesario.

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

La información documentada deberá estar disponible como evidencia de:

f) la naturaleza de las no conformidades y cualquier acción posterior 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 enumerados en [Cuadro A.1](#) se derivan directamente y están alineados con los enumerados en ISO/IEC 27002:2022^[1], Cláusulas 5 a 8, y se utilizará en contexto con [6.1.3](#).

Tabla A.1 — Controles de seguridad de la información

5	Controles organizacionales	
5.1	Políticas de seguridad de la información	<p>Control</p> <p>La política de seguridad de la información y las políticas específicas del tema deben ser definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si ocurren cambios significativos.</p>
5.2	Roles y responsabilidades de seguridad de la información	<p>Control</p> <p>Los roles y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.</p>
5.3	Segregación de deberes	<p>Control</p> <p>Deben separarse los deberes conflictivos y las áreas conflictivas de responsabilidad.</p>
5.4	responsabilidades de gestión	<p>Control</p> <p>La gerencia debe exigir 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.</p>
5.5	Contacto con autoridades	<p>Control</p> <p>La organización deberá establecer y mantener contacto con las autoridades pertinentes.</p>
5.6	Contacto con grupos de interés especial	<p>Control</p> <p>La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.</p>
5.7	Inteligencia de amenazas	<p>Control</p> <p>La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas.</p>
5.8	Seguridad de la información en la gestión de proyectos.	<p>Control</p> <p>La seguridad de la información se integrará en la gestión de proyectos.</p>
5.9	Inventario de información y otros activos asociados	<p>Control</p> <p>Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.</p>
5.10	Uso aceptable de la información y otros activos asociados	<p>Control</p> <p>Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.</p>
5.11	Devolución de activos	<p>Control</p> <p>El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.</p>

Cuadro A.1(continuado)

5.12	Clasificación de la información	Control La información se clasificará 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 información	Control Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo 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 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 establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio.
5.16	Gestión de identidad	Control Se gestionará el ciclo de vida completo de las identidades.
5.17	Información de autenticación	Control La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido 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 proporcionarse, revisarse, modificarse y eliminarse 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 las relaciones 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 de seguridad de la información pertinentes se establecerán y acordarán 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 monitorear, 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 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.

Cuadro A.1(continuado)

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 clasificarán 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	Aprender de los incidentes de seguridad de la información	Control El conocimiento obtenido de los incidentes de seguridad de la información se utilizará 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 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 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, reglamentarios y contractuales	Control Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes 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 publicación no autorizada.
5.34	Privacidad y protección de la información de identificación personal (PII)	Control La organización deberá identificar y cumplir los requisitos relacionados con 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 la seguridad de la información.	Control El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Control El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente.
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.

Cuadro A.1(continuado)

6	Controles de personas	
6.1	Poner en pantalla	<p>Control</p> <p>Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y la riesgos percibidos.</p>
6.2	Términos y condiciones de empleo	<p>Control</p> <p>Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.</p>
6.3	Concientización, educación y capacitación en seguridad de la información	<p>Control</p> <p>El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.</p>
6.4	Proceso Disciplinario	<p>Control</p> <p>Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.</p>
6.5	Responsabilidades después de la terminación o cambio de empleo	<p>Control</p> <p>Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas.</p>
6.6	Acuerdos de confidencialidad o no divulgación	<p>Control</p> <p>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 relevantes.</p>
6.7	Trabajo remoto	<p>Control</p> <p>Se implementarán 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.</p>
6.8	Informes de eventos de seguridad de la información	<p>Control</p> <p>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.</p>
7	Controles físicos	
7.1	Perímetros físicos de seguridad	<p>Control</p> <p>Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.</p>
7.2	Entrada física	<p>Control</p> <p>Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.</p>
7.3	Asegurar oficinas, salas e instalaciones	<p>Control</p> <p>Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.</p>
7.4	Monitoreo de seguridad física	<p>Control</p> <p>Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.</p>

Cuadro A.1(continuado)

7.5	Protección contra amenazas físicas y ambientales.	Control Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
7.6	Trabajar en áreas seguras	Control Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
7.7	Escritorio despejado y pantalla despejada	Control Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
7.8	Emplazamiento y protección de equipos	Control El equipo se colocará de forma segura y protegida.
7.9	Seguridad de los activos fuera de las instalaciones	Control Se protegerán los activos fuera del sitio.
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 y los requisitos de manipulación de la organización.
7.11	Utilidades de apoyo	Control Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
7.12	seguridad del cableado	Control Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.
7.13	Mantenimiento de equipo	Control El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación segura o reutilización de equipos	Control Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobreescrito de forma segura antes de su eliminación o reutilización.
8	Controles tecnológicos	
8.1	Dispositivos de punto final de usuario	Control Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
8.2	Derechos de acceso privilegiado	Control La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.
8.3	Restricción de acceso a la información	Control El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el 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 bibliotecas de software se gestionará adecuadamente.

Cuadro A.1(continuado)

8.5	Autenticación segura	Control Las tecnologías y procedimientos de autenticación segura se implementarán 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 El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.
8.7	Protección contra malware	Control La protección contra el malware se implementará y respaldará mediante la 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 los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
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 de fuga de datos	Control Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Copia de seguridad de la información	Control Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
8.14	Redundancia de las instalaciones de procesamiento de información	Control Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15	Inicio sesión	Control Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.
8.16	Actividades de seguimiento	Control Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas 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 estar sincronizados con las fuentes de tiempo aprobadas.

Cuadro A.1(continuado)

8.18	Uso de programas de utilidad privilegiados	Control El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.
8.19	Instalación de software en sistemas operativos	Control Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
8.20	Seguridad en redes	Control Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.
8.21	Seguridad de los servicios de red.	Control Se identificarán, implementarán y controlarán 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 web	Control El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	Control Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	Control Se establecerán y aplicarán 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	Principios de arquitectura e ingeniería 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 Los principios de codificación segura se aplicarán al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación.	Control Los procesos de pruebas de seguridad se definirán e implementarán 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 del cambio	Control Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.
8.33	Información de prueba	Control La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.

Cuadro A.1(*continuado*)

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/CEI 27002:2022, *Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información*
- [2] ISO/CEI 27003, *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información sistemas — Orientación*
- [3] ISO/CEI 27004, *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información — Seguimiento, medición, análisis y evaluación*
- [4] ISO/CEI 27005, *Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de los riesgos de seguridad de la información*
- [5] ISO 31000:2018, *Gestión de riesgos — Directrices*

