INTERNATIONAL STANDARD
ISO/IEC 27001
3a Ed, 2022

Seguridad de la Información, Ciberseguridad y Protección de la Privacidad — Sistemas de gestión de la Seguridad de la Información — Requisitos

Introducción

0.1 General

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 esté integrado 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 propios de la 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.

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. ***La exclusión de cualquiera de los requisitos especificados en las 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/IEC 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 en línea de ISO: 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 obligaciones contractuales.

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 mencionadas en 4.1;

b) los requisitos mencionados en 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 la 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 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 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 rendimiento del 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 considerar los problemas mencionados en 4.1 y los requisitos mencionados en 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) se materializaran;

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) anterior con los del Anexo A y verificar que no se hayan omitido los controles necesarios;

NOTA 2 El Anexo A contiene una lista de posibles controles de seguridad de la información. Se dirige a los usuarios de este documento al 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 el Anexo A no son exhaustivos y se pueden incluir controles de seguridad de la información adicionales si es necesario.

d) producir una Declaración de Aplicabilidad que contenga:

— los controles necesarios (ver 6.1.3 b) yc));

— justificación de su inclusión;

— si se aplican o no los controles necesarios; y

— la justificación para excluir cualquiera de los controles del Anexo A.

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 los principios y lineamientos genéricos proporcionados en ISO 31000[5].

6.2 Objetivos de seguridad de la información y planificación para lograrlos

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, la tutoría o la 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 deben 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 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

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 medios (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 solo 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) Conforme 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 la mejora continua.

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 la Tabla A.1 se derivan directamente y están alineados con los enumerados en ISO/IEC 27002:2022[1], Cláusulas 5 a 8, y se utilizarán en contexto con 6.1.3.

Cuadro A.1. Controles de seguridad de la información

5	**Controles organizativos**	
5.1	Políticas de seguridad de la información	**Control** La política de seguridad de la información y las políticas específicas del tema serán 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.
5.2	Funciones y responsabilidades de 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	Separación de funciones	**Control** Las funciones conflictivas y los ámbitos de responsabilidad conflictivos se separarán.
5.4	Responsabilidades de gestión	**Control** La gerencia requerirá que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos específicos del tema de la organización.
5.5	Contacto con las autoridades	**Control** La organización debe establecer y mantener contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especial	**Control** La organización debe establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.

5.7	Inteligencia de amenazas	**Control** La información relativa a las amenazas a la seguridad de la información se recopilará y analizará para producir información sobre amenazas.
5.8	Seguridad de la información en la gestión de proyectos	**Control** La seguridad de la información se integrará en la gestión del proyecto.
5.9	Inventario de información y otros activos asociados	**Control** Se elaborará y mantendrá un inventario de la información y otros activos asociados, incluidos los propietarios.
5.10	Uso aceptable de la información y otros activos asociados	**Control** Se identificarán, documentarán y aplicarán normas para el uso aceptable y los procedimientos para el manejo de la información y otros activos asociados.
5.11	Devolución de activos	**Control** El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización en su poder al cambiar o terminar su empleo, contrato o acuerdo.
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, integridad, disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	Etiquetado de la información	**Control** Se elaborará y aplicará un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización.
5.14	Transferencia de información	**Control** Las reglas, procedimientos o acuerdos de transferencia de información deben estar en su lugar 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 sobre la

		base de los requisitos comerciales y de seguridad de la información.
5.16	Gestión de identidades	**Control** Se gestionará todo el ciclo de vida 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 tratamiento adecuado de la información de autenticación.
5.18	Derechos de acceso	**Control** Los derechos de acceso a la información y otros activos asociados se aprovisionarán, revisarán, modificarán y eliminarán de acuerdo con la política y las reglas específicas del tema de la organización sobre el control de acceso.
5.19	Seguridad de la información en las relaciones con los proveedores	**Control** Se definirán e implementarán 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 dentro de los acuerdos con proveedores	**Control** Los requisitos pertinentes de seguridad de la información 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 las tecnologías de la información y la comunicación (TIC)	**Control** Se definirán y aplicarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.
5.22	Monitoreo, revisión y gestión del cambio de los servicios de los proveedores	**Control** La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio 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 establecerán 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 gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
5.25	Evaluación y decisión sobre eventos de seguridad de la información	**Control** La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	**Control** Los incidentes de seguridad de la información se responderán de acuerdo con los procedimientos documentados.
5.27	Aprender de los incidentes de seguridad de la información	**Control** Los conocimientos adquiridos en los incidentes de seguridad de la información se utilizarán para reforzar y mejorar los controles de seguridad de la información.
5.28	Obtención de pruebas	**Control** La organización debe establecer e implementar procedimientos para la identificación, recopilación, 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 apropiado durante la interrupción.
5.30	Preparación de las TIC para la continuidad de las actividades	**Control** La preparación para las TIC se planificará, aplicará, mantendrá y probará sobre la base de los objetivos de continuidad de las actividades 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 aplicará procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	Protección de registros	**Control** Los registros estarán protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.
5.34	Privacidad y protección de la información de identificación personal (PII)	**Control** La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales.
5.35	Examen 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, reglas y estándares para la seguridad de la información	**Control** El cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos del tema se revisarán regularmente.
5.37	Procedimientos operativos documentados	**Control** Los procedimientos operativos de las instalaciones de tratamiento de la información se documentarán y se pondrán a disposición del personal que los necesite.
6	**Controles de personas**	
6.1	Chequeo	**Control** Las verificaciones de antecedentes de todos los candidatos a convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continúa teniendo en cuenta las leyes, regulaciones y ética aplicables y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
6.2	Términos y condiciones de empleo	**Control** Los acuerdos contractuales de empleo establecerán las responsabilidades del personal y de la organización para la seguridad

		de la información.
6.3	Concienciación, educación y capacitación sobre seguridad de la información	**Control** El personal de la organización y las partes interesadas pertinentes recibirán concienciación, educación y capacitación apropiadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea relevante para su función laboral.
6.4	Proceso disciplinario	**Control** Se formalizará y comunicará un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.
6.5	Responsabilidades después de la terminación o cambio de empleo	**Control** Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o cambio de empleo se definirán, harán cumplir y comunicarán 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 en materia de protección de la información serán identificados, documentados, revisados periódicamente y firmados por el personal y otras partes interesadas pertinentes.
6.7	Trabajo remoto	**Control** Las medidas de seguridad se implementarán cuando el personal trabaje de forma remota para proteger la información accedida, procesada o almacenada fuera de las instalaciones de la organización.
6.8	Informes de eventos de seguridad de la información	**Control** La organización debe proporcionar un mecanismo para que el personal informe los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados de manera oportuna.
7	**Controles físicos**	
7.1	Perímetros de seguridad física	**Control** Los perímetros de seguridad se definirán y utilizarán para proteger las

		zonas que contengan información y otros activos asociados.
7.2	Entrada física	**Control** Las zonas seguras estarán protegidas por controles de entrada y puntos de acceso adecuados.
7.3	Asegurar oficinas, habitaciones e instalaciones	**Control** Se diseñará y aplicará la seguridad física de las oficinas, salas e instalaciones.
7.4	Monitoreo de seguridad física	**Control** Los locales serán monitoreados continuamente para detectar el acceso físico no autorizado.
7.5	Protección contra amenazas físicas y ambientales	**Control** Se diseñará y aplicará la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionales a las infraestructuras.
7.6	Trabajar en zonas seguras	**Control** Se diseñarán y aplicarán medidas de seguridad para trabajar en zonas seguras.
7.7	Escritorio claro y pantalla clara	**Control** Se definirán y aplicarán adecuadamente normas de escritorio claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas para las instalaciones de tratamiento de la información.
7.8	Emplazamiento y protección de equipos	**Control** El equipo deberá estar colocado de forma segura y protegida.
7.9	Seguridad de los activos fuera de las instalaciones	**Control** Los activos externos estarán protegidos.
7.10	Medios de almacenamiento	**Control** Los medios de almacenamiento se gestionarán durante todo 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 tratamiento de la información deberán estar protegidas contra fallos de suministro eléctrico y otras interrupciones causadas por fallos en los servicios públicos de apoyo.
7.12	Seguridad del cableado	**Control** Los cables que transporten energía, datos o servicios de información de apoyo estarán protegidos contra interceptaciones, interferencias o daños.
7.13	Mantenimiento de equipos	**Control** El equipo deberá mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.
7.14	Eliminación segura o reutilización del equipo	**Control** Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que los datos confidenciales 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 de punto final de usuario	**Control** Se protegerá la información almacenada, tratada o accesible a través de dispositivos de punto final de usuario.
8.2	Derechos de acceso privilegiados	**Control** Se restringirá y gestionará la asignación y el uso de derechos de acceso privilegiados.
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 de control de acceso establecida sobre temas específicos.
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.
8.5	Autenticación segura	**Control** Las tecnologías y procedimientos de autenticación segura se implementarán sobre la base de las restricciones de acceso a la

		información y la política de control de acceso específica del tema.
8.6	Gestión de la capacidad	**Control** El uso de los recursos se supervisará y ajustará en función de las necesidades de capacidad actuales y previstas.
8.7	Protección contra malware	**Control** La protección contra el malware se implementará y estará respaldada por un conocimiento adecuado del usuario.
8.8	Gestión de vulnerabilidades técnicas	**Control** Se obtendrá información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evaluará la exposición de la organización a dichas vulnerabilidades y se tomarán las medidas apropiadas.
8.9	Gestión de la configuración	**Control** Se establecerán, documentarán, aplicarán, supervisarán y revisarán las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes.
8.10	Eliminación de información	**Control** La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria.
8.11	Enmascaramiento de datos	**Control** El enmascaramiento de datos se utilizará de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas específicas de temas relacionados, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
8.12	Prevención de fuga de datos	**Control** Se aplicarán medidas de prevención de fuga de datos 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 acordada sobre copias de seguridad.

8.14	Redundancia de instalaciones de procesamiento de información	**Control** Las instalaciones de tratamiento de la información se implantarán con una redundancia suficiente para cumplir los requisitos de disponibilidad.
8.15	Registro	**Control** Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallos y otros eventos relevantes.
8.16	Actividades de supervisión	**Control** Se supervisarán las redes, los sistemas y las aplicaciones para detectar comportamientos anómalos y se tomarán las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización del reloj	**Control** Los relojes de los sistemas de procesamiento de información utilizados por la organización deben sincronizarse con las fuentes de tiempo aprobadas.
8.18	Uso de programas de utilidad privilegiados	**Control** El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.
8.19	Instalación de software en sistemas operativos	**Control** Se implementarán procedimientos y medidas para administrar de forma segura la instalación de software en los sistemas operativos.
8.20	Seguridad de redes	**Control** Las redes y los dispositivos de red deben estar protegidos, gestionados y controlados para proteger la información en los sistemas y aplicaciones.
8.21	Seguridad de los servicios de red	**Control** Se identificarán, aplicarán y supervisarán 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 se separarán en las redes de la organización.

8.23	Filtrado web	**Control** El acceso a sitios web externos se gestionará para reducir la exposición a contenidos maliciosos.
8.24	Uso de criptografía	**Control** Se definirán y aplicarán normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	**Control** Se establecerán y aplicarán normas para el desarrollo seguro de programas informáticos y sistemas.
8.26	Requisitos de seguridad de las aplicaciones	**Control** Los requisitos de seguridad de la información se identificarán, especificarán y aprobarán al desarrollar o adquirir aplicaciones.
8.27	Arquitectura de sistemas seguros y principios de ingeniería	**Control** Los principios para la ingeniería de sistemas seguros se establecerán, documentarán, mantendrán y aplicarán a 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 y aplicarán en el ciclo de vida del desarrollo.
8.30	Desarrollo externalizado	**Control** La organización dirigirá, supervisará y revisará las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	Separación de entornos de desarrollo, prueba y producción	**Control** Los entornos de desarrollo, ensayo y producción deberán estar separados y protegidos.
8.32	Gestión del cambio	**Control** Los cambios en las instalaciones de tratamiento de la información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.

8.33	Información de la prueba	**Control** La información del ensayo se seleccionará, protegerá y gestionará 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 impliquen la evaluación de los sistemas operativos se planificarán y acordarán entre el evaluador y la dirección apropiada.

Bibliografía

[1] ISO/IEC 27002:2022, Seguridad de la información, *ciberseguridad y protección de la privacidad — Controles de seguridad de la información*

[2] ISO/IEC 27003, Tecnología de la información — *Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Guía*

[3] ISO/IEC 27004, Tecnología de la información — Técnicas de seguridad — Gestión de la *seguridad de la información — Monitoreo, medición, análisis y evaluación*

[4] ISO/IEC 27005, *Seguridad de la información, ciberseguridad y protección de la privacidad — Guía sobre la gestión de los riesgos de seguridad de la información*

ISO 31000:2018, *Gestión de riesgos — Directrices*