

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

E: Information security, cybersecurity and privacy protection.
Informationsecurity management systems. Requirements

CORRESPONDENCIA: esta Norma Técnica Colombiana es idéntica (IDT) por traducción (IDT) de la norma ISO/IEC 27001:2022 y está cubierta por los derechos de autor y otros derechos de propiedad intelectual de la IEC, según el acuerdo de licencia con esta entidad.

DESCRIPTORES: sistemas de gestión; gestión; seguridad de la información; técnicas de seguridad; ciberseguridad; controles de seguridad.

I.C.S.: 03.100.70; 35.030

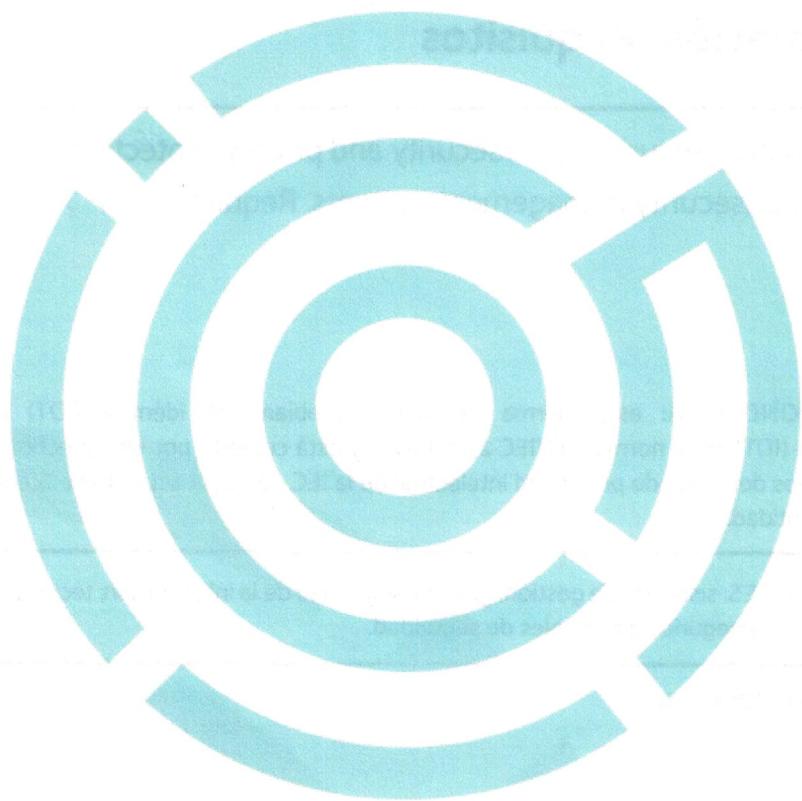


© ICONTEC 2022

Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida o utilizada en cualquier forma o por cualquier medio, electrónico o mecánico incluyendo fotocopiado y microfilmación, sin permiso por escrito del editor.

Editada por ICONTEC. Numeral 14237 Bogotá, D.C. - Tel. (571) 6078888

Prohibida su reproducción | Editada 2022-11-09



PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación (**ICONTEC**) es el organismo nacional de normalización, según el Decreto 1595 de 2015.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

Se llama la atención sobre la posibilidad de que algunos elementos de este documento pueden ser objeto de derechos de patente. **ICONTEC** no asume la responsabilidad por la identificación de dichas patentes, o por la documentación que se haya aportado que goza de esta protección legal.

La norma NTC-ISO/IEC 27001 (Segunda actualización) fue elaborada por el CTN 181 Gestión de la tecnología de la Información y ratificada por el Consejo Directivo de 2022-11-09.

Este documento está sujeto a ser revisado en cualquier momento con el objeto de que responda a las necesidades y exigencias actuales. Se invita a los usuarios de este documento a presentar sus solicitudes de revisión a **ICONTEC**; sus comentarios serán puestos a consideración del comité técnico responsable del estudio de este tema.

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

	Página
INTRODUCCIÓN.....	I
0.1 Generalidades	I
0.2 Compatibilidad con otras normas de Sistemas de Gestión	I
1. OBJETO Y CAMPO DE APLICACIÓN	1
2. REFERENCIAS NORMATIVAS	1
3. TÉRMINOS Y DEFINICIONES	1
4. CONTEXTO DE LA ORGANIZACIÓN	2
4.1 Comprensión de la organización y su contexto	2
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.....	2
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	3
5.1 Liderazgo y compromiso.....	3
5.2 Política	3
5.3 Roles, responsabilidades y autoridades de la organización	4

Página

6.	PLANIFICACIÓN	4
6.1	Acciones para abordar los riesgos y las oportunidades	4
6.2	Objetivos de seguridad de la información y planificación para alcanzarlos	6
6.3	Planificación de los cambios	7
7.	APOYO	7
7.1	Recursos	7
7.2	Competencia.....	8
7.3	Toma de conciencia.....	8
7.4	Comunicación	8
7.5	Información documentada	8
8.	OPERACIÓN	10
8.1	Planificación y control de la operación	10
8.2	Evaluación de los riesgos para la seguridad de la información	10
8.3	Tratamiento de los riesgos para la seguridad de la información.....	10
9.	EVALUACIÓN DEL DESEMPEÑO	10
9.1	Seguimiento, medición, análisis y evaluación	10
9.2	Auditoría interna	11
9.3	Revisión por la dirección	12
10.	MEJORA.....	13

Página

10.1 Mejora continua.....	13
10.2 No conformidad y acción correctiva	13

ANEXOS

ANEXOS A (Normativo) REFERENCIA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN	14
ANEXOS B (Informativo) CAMBIOS ENTRE LA VERSIÓN ANTERIOR DE LA NTC-ISO/IEC 27001 Y LA PRESENTE ACTUALIZACIÓN.....	23
BIBLIOGRAFÍA.....	23
DOCUMENTO DE REFERENCIA.....	25

INTRODUCCIÓN

0.1 Generalidades

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

El sistema de gestión de seguridad de la información preserva la confidencialidad, la integridad y la 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 seguridad de la información forme parte y se integre en los procesos de la organización y en la estructura general de gestión, 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 amplíe, 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 los requisitos de seguridad de la información de la propia organización.

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

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

0.2 Compatibilidad con otras normas de Sistemas de Gestión

Este documento aplica la estructura de alto nivel, los títulos idénticos de los numerales, 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 tanto mantiene la compatibilidad con otras normas de sistemas de gestión que han adoptado el Anexo SL.

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

**SEGURIDAD DE LA INFORMACIÓN,
CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD.
SISTEMAS DE GESTIÓN DE LA SEGURIDAD
DE LA INFORMACIÓN.
REQUISITOS**

1. OBJETO Y CAMPO DE APLICACIÓN

Este documento especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en el contexto de la organización. Este documento también incluye los 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 pretenden ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. La exclusión de cualquiera de los requisitos especificados en los numerales 4 a 10 no es aceptable cuando una organización declara conformidad con este documento.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos normativos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos para este documento. Para las referencias fechadas, se aplica únicamente la edición citada. Para referencias no fechadas, se aplica la última edición del documento referenciado (incluida cualquier corrección).

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

3. TÉRMINOS Y DEFINICIONES

Para los efectos de este documento, se aplican los términos y las definiciones dadas en la norma ISO/IEC 27000.

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

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

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y su contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información.

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

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar

- a) las partes interesadas que son pertinentes para el sistema de gestión de seguridad de la información;
- b) los requisitos pertinentes de estas partes interesadas;
- c) cuáles de estos requisitos se abordarán 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 seguridad de la información para establecer su alcance.

Al determinar este alcance, la organización debe considerar

- a) las cuestiones externas e internas mencionadas en el numeral 4.1;
- b) los requisitos mencionados en el numeral 4.2;
- c) las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de la información

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

5. LIDERAZGO

5.1 Liderazgo y compromiso

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

- a) asegurar que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y son compatibles con la dirección estratégica de la organización;
- b) asegura la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;
- c) asegurar la disponibilidad de los recursos necesarios para el sistema de gestión de seguridad de la información
- d) comunicar la importancia de una gestión eficaz de la seguridad de la información y de la conformidad con los requisitos del sistema de gestión de seguridad de la información
- e) asegurar que el sistema de gestión de 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 seguridad de la información;
- g) promover la mejora continua; y
- h) apoyar a otros roles de gestión pertinentes para que demuestren su liderazgo en lo que respecta a sus áreas de responsabilidad.

NOTA La referencia al "negocio" en este documento puede interpretarse de forma amplia para significar aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

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

- a) sea adecuada al propósito de la organización;
- b) incluya objetivos de seguridad de la información (véase el numeral 6.2) o proporcione el marco de referencia para establecer objetivos de seguridad de la información;
- c) incluya el compromiso para satisfacer los requisitos aplicables relacionados con la seguridad de la información;
- d) incluye el compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información debe:

- e) estar disponible como información documentada;
- f) ser comunicada dentro de la organización;
- g) estar disponible para las partes interesadas, según corresponda.

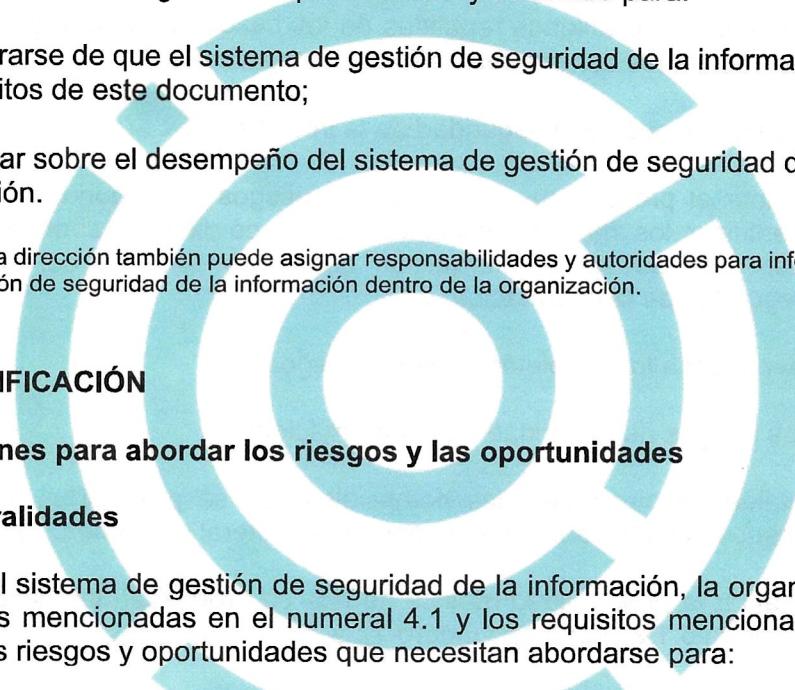
5.3 Roles, responsabilidades y autoridades de la organización

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

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) asegurarse de que el sistema de gestión de seguridad de la información es conforme con 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 del sistema de gestión de seguridad de la información dentro de la organización.



6. PLANIFICACIÓN

6.1 Acciones para abordar los riesgos y las oportunidades

6.1.1 Generalidades

Al planificar el sistema de gestión de seguridad de la información, la organización debe considerar las cuestiones mencionadas en el numeral 4.1 y los requisitos mencionados en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan abordarse para:

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

La organización debe planificar:

- d) las acciones para abordar estos riesgos y oportunidades; y
- e) la manera de:
 - 1) integrar e implementar las acciones en sus procesos del sistema de gestión de seguridad de la información; y

- 2) evaluar la eficacia 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) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan
 - 1) los criterios de aceptación del riesgo; y
 - 2) los criterios para la realización de evaluaciones de riesgos para la seguridad de la información;
- b) asegure que las evaluaciones repetidas de los riesgos para la seguridad de la información produzcan resultados coherentes, válidos y comparables
- c) identifique los riesgos de la 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 de los riesgos;
- d) analiza los riesgos de seguridad de la información:
 - 1) evalúe las consecuencias potenciales que se producirían si se materializaran los riesgos identificados en el numeral 6.1.2, literal c), número 1);
 - 2) evaluar la probabilidad realista de que se produzcan los riesgos identificados en el numeral 6.1.2, literal c), número 1); y
 - 3) determinar los niveles de riesgo;
- e) valore los riesgos para la seguridad de la información:
 - 1) comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en el numeral 6.1.2, literal a); y
 - 2) priorizar los riesgos analizados para su tratamiento.

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

6.1.3 Tratamiento de los 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 las opciones de tratamiento de riesgos de seguridad de la información adecuadas, teniendo en cuenta los resultados de la evaluación de riesgos
- b) determinar todos los controles necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA 1 Las organizaciones pueden diseñar los controles necesarios o identificarlos a partir de cualquier fuente.

- c) comparar los controles determinados en el numeral 6.1.3, literal b), anterior con los del anexo A y verificar que no se ha omitido ningún control necesario;

NOTA 2 El Anexo A contiene una lista de posibles controles de seguridad de la información. Los usuarios de este documento son dirigidos al Anexo A para asegurarse de que no se ha omitido ningún control de seguridad de la información necesario.

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

- d) producir una declaración de aplicabilidad que contenga
 - los controles necesarios (véase el numeral 6.1.3, literales b) y c))
 - la justificación de su inclusión
 - si los controles necesarios están implementados o no; y
 - la justificación para excluir cualquiera de los controles del Anexo A.
- e) formular un plan de tratamiento de los riesgos de seguridad de la información; y
- f) obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la seguridad de la información

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

NOTA 4 El proceso de evaluación y tratamiento de los riesgos de seguridad de la información en este documento se alinea con los principios y directrices genéricas proporcionadas en la norma 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 deben:

- a) Ser coherentes con la política de seguridad de la información;
- b) ser medibles (si es posible);
- c) tener en cuenta los requisitos de seguridad de la información aplicables y los resultados de la evaluación y el tratamiento de los riesgos
- d) ser monitoreados;
- e) ser comunicados;
- f) actualizarse cuando sea necesario;
- g) estar disponibles como información documentada.

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

Cuando se hace la planificación para lograr sus objetivos de seguridad de la información, la organización debe determinar:

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

6.3 Planificación de los cambios

Cuando la organización determine la necesidad de realizar cambios al sistema de gestión de seguridad de la información, éstos se llevarán a cabo de forma planificada.

7. APOYO

7.1 Recursos

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

7.2 Competencia

La organización debe:

- a) determinar la competencia necesaria de la(s) persona(s) que realice(n) bajo su control un trabajo que afecte al desempeño de la seguridad de la información;
- b) asegurarse de que estas personas son competentes sobre la base de una educación, formación o experiencia adecuadas;
- c) cuando proceda, tomar medidas para adquirir la competencia necesaria y evaluar la eficacia de las medidas adoptadas; y
- d) conservar la información documentada adecuada como evidencia de la competencia.

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

7.3 Toma de conciencia

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

- a) la política de seguridad de la información;
- b) su contribución a la eficiencia del sistema de gestión de seguridad de la información, incluidos los beneficios de la mejora del desempeño de la seguridad de la información; y
- c) las implicaciones de la no conformidad con los requisitos del sistema de gestión de seguridad de la información.

7.4 Comunicación

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

- a) sobre qué comunicar;
- b) cuándo comunicar;
- c) con quién comunicarse;
- d) cómo comunicar.

7.5 Información documentada

7.5.1 Generalidades

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

- a) la información documentada requerida por este documento; y

- b) la información documentada que la organización determine como necesaria para la eficiencia del sistema de gestión de 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

Cuando se crea y actualiza información documentada, la organización debe asegurar apropiadamente:

- a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);
- b) el formato (por ejemplo, el idioma, la versión del software, los gráficos) y el medio (por ejemplo, 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 debe ser controlada para asegurarse de que:

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

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

- c) distribución, acceso, recuperación y uso;
- d) el almacenamiento y la preservación, incluida la preservación de la legibilidad
- e) control de cambios (por ejemplo, control de versiones); y
- f) retención y disposición.

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

NOTA El acceso puede implicar una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

8. OPERACIÓN

8.1 Planificación y control de la operación

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

- estableciendo criterios para los procesos;
- implementando control de los procesos de acuerdo con los criterios.

La información documentada debe estar disponible en la medida necesaria para tener confianza en que los procesos han sido ejecutados según lo planificado.

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

La organización debe asegurarse de que se controlan los procesos, productos o servicios suministrados externamente que sean pertinentes para el sistema de gestión de seguridad de la información.

8.2 Evaluación de los riesgos para la seguridad de la información

La organización debe realizar evaluaciones de los riesgos para la seguridad de la información a intervalos planificados o cuando se propongan o se produzcan cambios significativos, teniendo en cuenta los criterios establecidos en el numeral 6.1.2, literal 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 los riesgos para la seguridad de la información.

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

9. EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- a) a qué es necesario hacer seguimiento y ser medido, incluidos los procesos y controles de seguridad de la información;

- b) los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos
- c) cuándo se debe realizar el seguimiento y la medición
- d) quién debe realizar el seguimiento y la medición;
- e) cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;
- f) quién analizará y evaluará estos resultados.

Se debe disponer de información documentada como evidencia de los resultados.

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

- a) es conforme con:
 - 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 eficazmente.

9.2.2 Programa de auditoría interna

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

Al establecer el programa o programas de auditoría interna, la organización debe considerar la importancia de los procesos involucrados y los resultados de las auditorías anteriores.

La organización debe:

- a) definir los criterios de auditoría y el alcance de cada auditoría;
- b) seleccionar a los auditores y realizar auditorías que aseguren la objetividad e imparcialidad del proceso de auditoría
- c) asegurarse de que los resultados de las auditorías se comunican a la dirección pertinente;

Se debe disponer de información documentada como evidencia de la implementación del (los) programa (s) de auditoría y de los resultados de auditoría.

9.3 Revisión por la dirección

9.3.1 Generalidades

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

9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe considerar:

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

9.3.3 Salidas de la revisión por la dirección

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

Se debe tener disponible información documentada como evidencia de los resultados de las revisiones por la dirección.

10. MEJORA

10.1 Mejora continua

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

10.2 No conformidad y acción correctiva

Cuando ocurra una no conformidad, la organización debe

- a) reaccionar ante la no conformidad y, cuando sea aplicable
 - 1) tomar acciones para controlarla y corregirla
 - 2) hacer frente a las consecuencias;
- b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante
 - 1) la revisión de la no conformidad
 - 2) determinando las causas de la no conformidad; y
 - 3) determinando si existen no conformidades similares, o que potencialmente podrían ocurrir;
- c) implementar cualquier acción necesaria;
- d) revisar la eficacia de cualquier acción correctiva tomada; y
- e) hacer cambios en el sistema de gestión de seguridad de la información, si es necesario.

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

La información documentada debe estar disponible como evidencia de:

- f) la naturaleza de las no conformidades y cualquier acción subsecuente tomada,
- g) los resultados de cualquier acción correctiva.

ANEXO A
(Normativo)

REFERENCIA A LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Los controles de seguridad de la información relacionados en la Tabla A.1 se derivan directamente y están alineados con aquellos citados en los numerales 5 a 8 de la GTC-ISO/IEC 27002:2022[1], y deben utilizarse en contexto con el numeral 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 asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurrán cambios significativos en la organización.</p>
5.2	Roles y responsabilidades en la Seguridad de la Información	<p>Control</p> <p>Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.</p>
5.3	Segregación de deberes	<p>Control</p> <p>Los deberes y áreas de responsabilidad en conflicto deberían segregarse.</p>
5.4	Responsabilidades de la dirección	<p>Control</p> <p>La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes.</p>
5.5	Contacto con las autoridades	<p>Control</p> <p>La organización debe establecer y mantener contacto con las autoridades pertinentes.</p>
5.6	Contacto con grupos de interés especial	<p>Control</p> <p>La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad</p>
5.7	Inteligencia de amenazas	<p>Control</p> <p>La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.</p>
5.8	Seguridad de la Información en la gestión de proyectos	<p>Control</p> <p>La seguridad de la información se debe integrar en la gestión de proyectos.</p>
5.9	Inventario de información y otros activos asociados	<p>Control</p> <p>Se debe elaborar y mantener un inventario de la 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 deben identificar, documentar y implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.</p>

Continúa...

Tabla A.1 (Continuación)

5	Controles organizacionales	
5.11	Devolución de activos	<p>Control</p> <p>El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.</p>
5.12	Clasificación de la información	<p>Control</p> <p>La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.</p>
5.13	Etiquetado de la información	<p>Control</p> <p>Se debe elaborar y implementar 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.</p>
5.14	Transferencia de información	<p>Control</p> <p>Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.</p>
5.15	Control de acceso	<p>Control</p> <p>Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información.</p>
5.16	Gestión de identidades	<p>Control</p> <p>Se debe gestionar el ciclo de vida completo de las identidades.</p>
5.17	Información de autenticación	<p>Control</p> <p>La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.</p>
5.18	Derechos de acceso	<p>Control</p> <p>Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso.</p>
5.19	Seguridad de la información en las relaciones con proveedores	<p>Control</p> <p>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.</p>
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	<p>Control</p> <p>Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor.</p>
5.21	Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)	<p>Control</p> <p>Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.</p>
5.22	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	<p>Control</p> <p>La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.</p>

Tabla A.1 (Continuación)

5	Controles organizacionales	
5.23	Seguridad de la información para el uso de servicios en la nube	<p>Control</p> <p>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.</p>
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	<p>Control</p> <p>La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.</p>
5.25	Evaluación y decisión sobre eventos de seguridad de la información	<p>Control</p> <p>La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.</p>
5.26	Respuesta a incidentes de seguridad de la información	<p>Control</p> <p>Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados.</p>
5.27	Aprender de los incidentes de seguridad de la información	<p>Control</p> <p>Los conocimientos adquiridos a partir de incidentes de seguridad de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información.</p>
5.28	Recopilación de evidencias	<p>Control</p> <p>La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.</p>
5.29	Seguridad de la información durante una interrupción	<p>Control</p> <p>La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.</p>
5.30	Preparación de las TIC para la continuidad de negocio	<p>Control</p> <p>La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.</p>
5.31	Requisitos legales, reglamentarios y contractuales	<p>Control</p> <p>Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.</p>
5.32	Derechos de propiedad intelectual	<p>Control</p> <p>La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual.</p>
5.33	Protección de registros	<p>Control</p> <p>Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados</p>

Tabla A.1 (Continuación)

5		Controles organizacionales
5.34	Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)	<p>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.</p>
5.35	Revisión independiente de la seguridad de la información	<p>Control El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.</p>
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	<p>Control El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.</p>
5.37	Procedimientos documentados operativos	<p>Control Los procedimientos operativos de las instalaciones de procesamiento e la información se debe documentar y poner a disposición del personal que los necesite.</p>
6		Controles de personas
6.1	Selección	<p>Control Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continua teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.</p>
6.2	Términos y condiciones de empleo	<p>Control Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.</p>
6.3	Conciencia de seguridad de la información, educación y formación	<p>Control El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas 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 pertinente para su función laboral.</p>
6.4	Proceso disciplinario	<p>Control Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.</p>
6.5	Responsabilidades después de la terminación o cambio de empleo	<p>Control Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal pertinente y a otras partes interesadas.</p>

Tabla A.1 (Continuación)

6	Controles de personas	
6.6	Acuerdos de confidencialidad o no divulgación	<p>Control</p> <p>Los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes.</p>
6.7	Trabajo remoto	<p>Control</p> <p>Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena 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 oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.</p>
7	Controles físicos	
7.1	Perímetros de seguridad física	<p>Control</p> <p>Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.</p>
7.2	Entrada física	<p>Control</p> <p>Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.</p>
7.3	Asegurar oficinas, habitaciones e instalaciones	<p>Control</p> <p>Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones.</p>
7.4	Monitoreo de la seguridad física	<p>Control</p> <p>Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.</p>
7.5	Protección contra amenazas físicas y ambientales	<p>Control</p> <p>Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.</p>
7.6	Trabajar en áreas seguras	<p>Control</p> <p>Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras.</p>
7.7	Escritorio y pantalla limpios	<p>Control</p> <p>Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información.</p>
7.8	Emplazamiento y protección de equipos	<p>Control</p> <p>El equipo debe estar situado de forma segura y protegida</p>
7.9	Seguridad de los activos fuera de las instalaciones	<p>Control</p> <p>Los activos externos deben estar protegidos.</p>

Tabla A.1 (Continuación)

7		Controles físicos
7.10	Medios de almacenamiento	<p>Control</p> <p>Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.</p>
7.11	Servicios públicos de apoyo	<p>Control</p> <p>Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.</p>
7.12	Seguridad del cableado	<p>Control</p> <p>Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños.</p>
7.13	Mantenimiento de equipos	<p>Control</p> <p>El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información.</p>
7.14	Disposición o reutilización segura de los equipos	<p>Control</p> <p>Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización.</p>
8		Controles tecnológicos
8.1	Dispositivos de punto final de usuario	<p>Control</p> <p>Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.</p>
8.2	Derechos de acceso privilegiado	<p>Control</p> <p>La asignación y el uso de los derechos de acceso privilegiado deben estar restringidos y gestionados.</p>
8.3	Restricción de acceso a la información	<p>Control</p> <p>El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.</p>
8.4	Acceso al código fuente	<p>Control</p> <p>El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente</p>
8.5	Autenticación segura	<p>Control</p> <p>Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.</p>
8.6	Gestión de la capacidad	<p>Control</p> <p>El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.</p>
8.7	Protección contra malware	<p>Control</p> <p>La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.</p>

Tabla A.1 (Continuación)

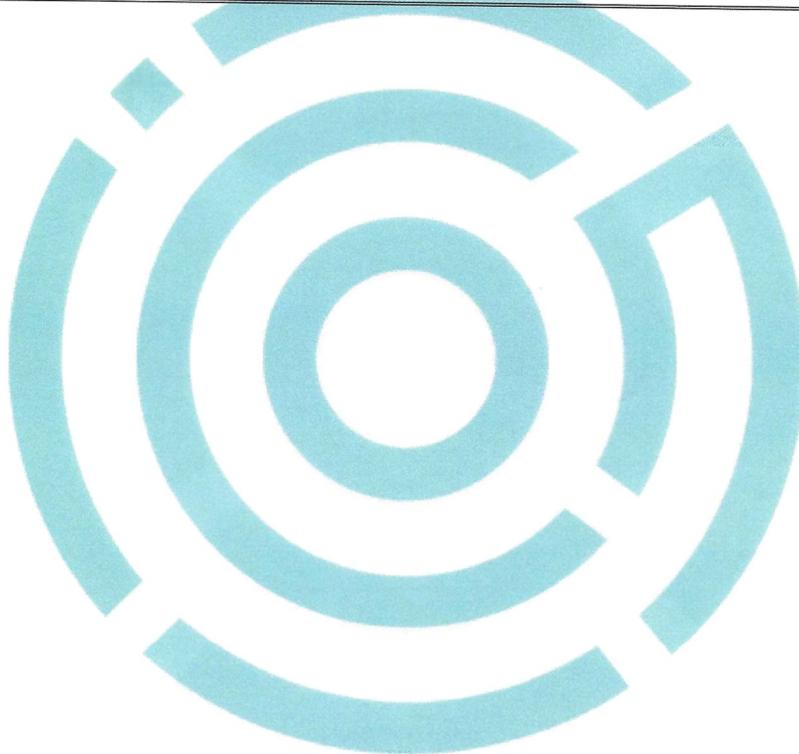
8	Controles tecnológicos	
8.8	Gestión de vulnerabilidades técnicas	<p>Control</p> <p>Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.</p>
8.9	Gestión de la configuración	<p>Control</p> <p>Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.</p>
8.10	Eliminación de información	<p>Control</p> <p>La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario</p>
8.11	Enmascaramiento de datos	<p>Control</p> <p>El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.</p>
8.12	Prevención de fugas de datos	<p>Control</p> <p>Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.</p>
8.13	Copia de seguridad de la información	<p>Control</p> <p>Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.</p>
8.14	Redundancia de las instalaciones de procesamiento de información	<p>Control</p> <p>Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad.</p>
8.15	Registro	<p>Control</p> <p>Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.</p>
8.16	Actividades de seguimiento	<p>Control</p> <p>Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.</p>
8.17	Sincronización de reloj	<p>Control</p> <p>Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas.</p>
8.18	Uso de programas de utilidad privilegiados	<p>Control</p> <p>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.</p>

Tabla A.1 (Continuación)

8	Controles tecnológicos	
8.19	Instalación de software en sistemas operativos	<p>Control</p> <p>Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.</p>
8.20	Seguridad de redes	<p>Control</p> <p>Las redes y los dispositivos de red deben estar asegurados, gestionados y controlados para proteger la información de los sistemas y las aplicaciones.</p>
8.21	Seguridad de los servicios de red	<p>Control</p> <p>Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.</p>
8.22	Segregación de redes	<p>Control</p> <p>Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.</p>
8.23	Filtrado web	<p>Control</p> <p>El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.</p>
8.24	Uso de la criptografía	<p>Control</p> <p>Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.</p>
8.25	Ciclo de vida de desarrollo seguro	<p>Control</p> <p>Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.</p>
8.26	Requisitos de seguridad de las aplicaciones	<p>Control</p> <p>Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.</p>
8.27	Arquitectura de sistemas seguros y principios de ingeniería	<p>Control</p> <p>Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y implementar a cualquier actividad de desarrollo de sistemas de información.</p>
8.28	Codificación segura	<p>Control</p> <p>Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.</p>
8.29	Pruebas de seguridad en el desarrollo y aceptación	<p>Control</p> <p>Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo.</p>
8.30	Desarrollo externalizado	<p>Control</p> <p>La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.</p>
8.31	Separación de entornos de desarrollo, evidencia y producción	<p>Control</p> <p>Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.</p>

Tabla A.1 (Final)

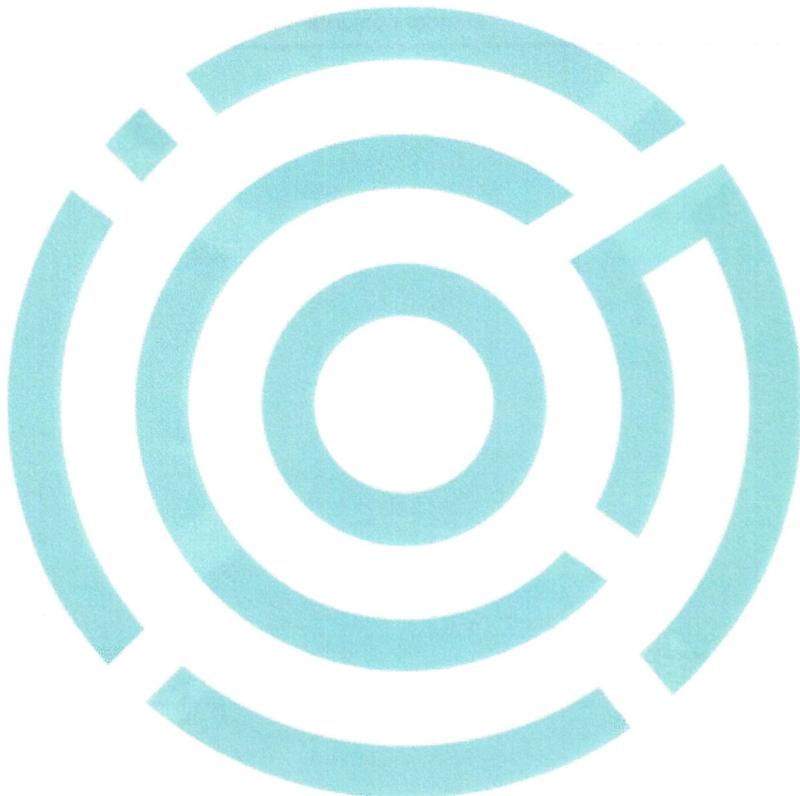
8	Controles tecnológicos	
8.32	Gestión del cambio	Control Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	Información de las pruebas	Control La información de las pruebas se debe seleccionar, proteger y gestionar 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 deben planificar y acordar conjuntamente entre el probador y la dirección adecuada



ANEXO B
(Informativo)

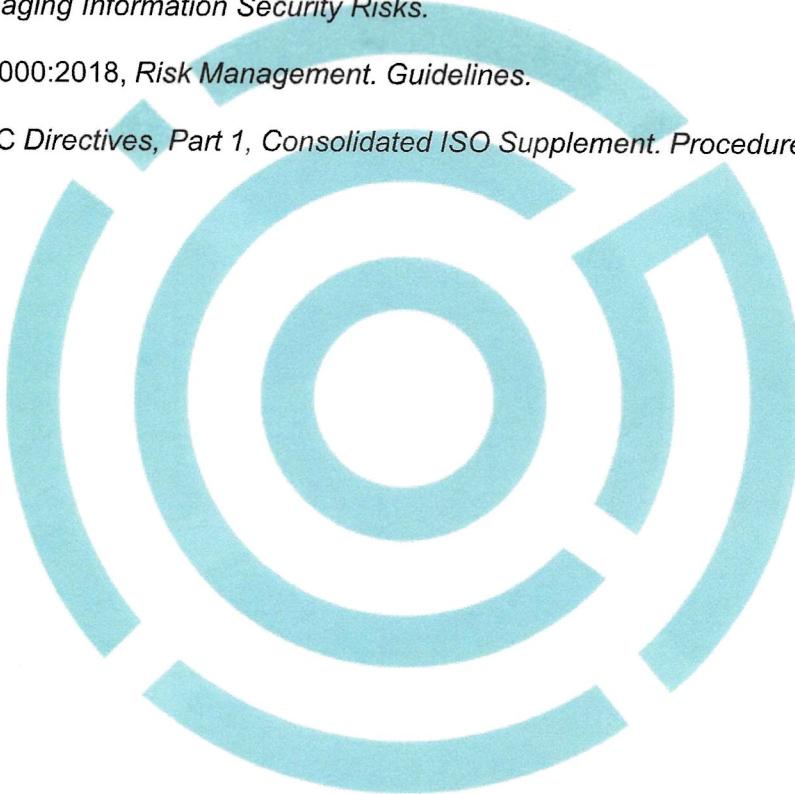
**CAMBIOS ENTRE LA VERSIÓN ANTERIOR DE LA NTC-ISO/IEC 27001 Y LA PRESENTE
ACTUALIZACIÓN**

La primera actualización de la norma incorpora las revisiones técnicas internacionales ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015. Además, el texto ha sido alineado con la estructura armonizada para normas de sistema de gestión y la GTC-ISO/IEC 27002 versión 2022.



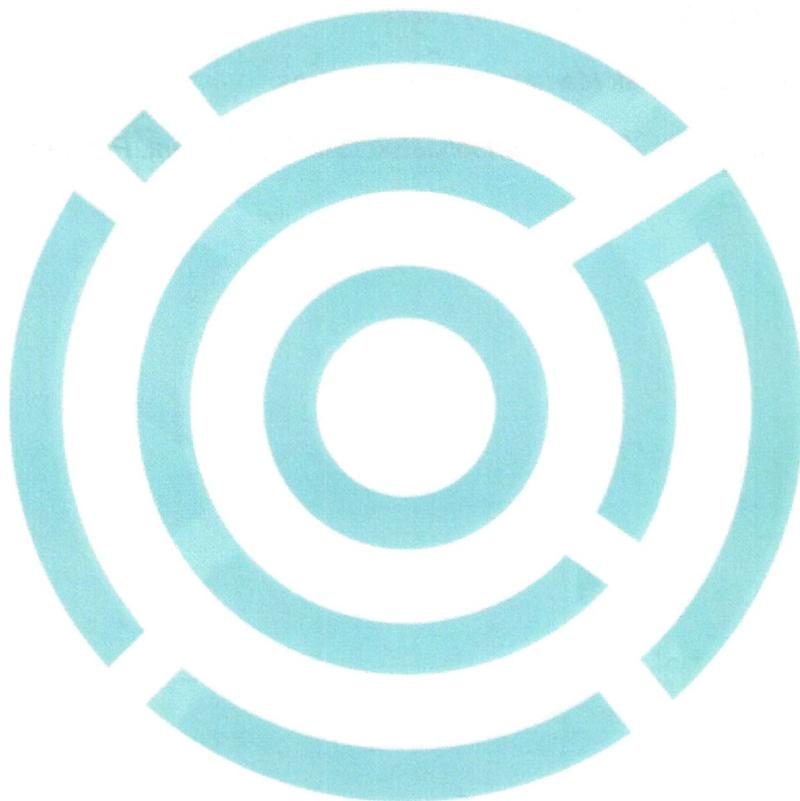
BIBLIOGRAFÍA

- [1] ISO/IEC 27002:2022, *Information Security, Cybersecurity and Privacy Protection. Information Security Controls*
- [2] ISO/IEC 27003, *Information Technology. Security Techniques. Information Security Management Systems. Guidance.*
- [3] ISO/IEC 27004, *Information Technology. Security Techniques. Information Security Management. Monitoring, Measurement, Analysis and Evaluation.*
- [4] ISO/IEC/DIS 27005, *Information Security, Cybersecurity and Privacy Protection. Guidance on Managing Information Security Risks.*
- [5] ISO 31000:2018, *Risk Management. Guidelines.*
- [6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement. Procedures Specific to ISO, 2012.*



DOCUMENTO DE REFERENCIA

INTERNATIONAL STANDARDIZATION ORGANIZATION/ INTERNATIONAL ELECTROTECHNICAL COMISION. *Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. Requirements.* Ginebra, 2022, 19p (ISO/IEC 27001:2022).



Colombia

Apartadó
apartado@icontec.org

Cali
cali@icontec.org

Ibagué
ibague@icontec.org

Armenia
armenia@icontec.org

Cartagena
cartagena@icontec.org

Neiva
neiva@icontec.org

Barranquilla
barranquilla@icontec.org

Cúcuta
cucuta@icontec.org

Pereira
pereira@icontec.org

Barrancabermeja
barrancabermeja@icontec.org

Manizales
manizales@icontec.org

Pasto
pasto@icontec.org

Bogotá
bogota@icontec.org

Medellín
medellin@icontec.org

Villavicencio
villavicencio@icontec.org

Bucaramanga
bucaramanga@icontec.org

Montería
monteria@icontec.org

Resto del mundo

Bolivia
bolivia@icontec.org

Costa Rica
costarica@icontec.org

Chile
chile@icontec.org

Ecuador
ecuador@icontec.org

El Salvador
elsalvador@icontec.org

Guatemala
guatemala@icontec.org

Honduras
honduras@icontec.org

México
mexico@icontec.org

Nicaragua
nicaragua@icontec.org

Panamá
panama@icontec.org

República Dominicana
republicadominicana@icontec.org

Perú
peru@icontec.org

Canales de atención al cliente:

Bogotá: **607 8888**

Resto del país: **01 8000 94 9000**

cliente@icontec.org

www.icontec.org