NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27007 2020

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 27) Lima, Perú

Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información

Information security, cybersecurity and privacy protection. Guidelines for information security management systems auditing

(EQV. ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing)

2020-11-12
3ª Edición

R.D. N° 032-2020-INACAL/DN. Publicada el 2020-11-26 Precio basado en 71 páginas
I.C.S.: 03.120.20; 35.030 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología de la información, técnica de seguridad, directrices para la auditoría, sistema de seguridad de la información, tecnología, información, seguridad, ciberseguridad

INACAL

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

ÍNDICE

página

PRÓLOGO

A. RESEÑA HISTÓRICA

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

A.2 La presente Norma Técnica Peruana fue elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a julio de 2020, utilizando como antecedente a la norma ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing.

A.3 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Dirección de Normalización -DN-, con fecha 2020-07-23, el PNTP-ISO/IEC 27007:2020**,** para su revisión y aprobación, siendo sometida a la etapa de discusión pública el 2020-09-07. No habiendo recibido observaciones, fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27007:2020 Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información**, 3ª Edición, el 26 de noviembre de 2020.

A.4 Esta tercera edición de la NTP-ISO/IEC 27007 reemplaza a la NTP-ISO/IEC 27007:2019 Tecnología de la información. Técnicas de seguridad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información. 2ª Edición. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurado de acuerdo con las Guías Peruanas GP 001:2016 y GP 002:2016.

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

Secretaría	GS1 PERU
Presidente	Ricardo Dioses

Secretaria	Mary Wong

ENTIDAD	**REPRESENTANTE**
Contraloría General de la República	Marco Bermúdez
Deloitte & Touche S. R. L.	Diana Lagos Pedro Torres
DMS Perú S. A. C.	Walter Eguizabel
GS1 PERÚ	Paola Carhuatanta Milagros Dávila
IBM del Perú S. A. C.	Ivan Ancco
Indecopi – Gerencia de Planeamiento Y Gestión Institucional	César Guerra
NSF INASSA S.A.C.	Raúl Miranda Karla León
ITSTK Perú S. A. C.	Belén Alvarado
Microsoft Perú S. R. L.	Fernando Gebara Héctor Figari
Ministerio de Economía y Finanzas – Oficina de Normalización Previsional – ONP	José Valdéz
Ministerio de Economía y Finanzas – Dirección General de Asuntos de Economía Internacional, Competencia y Productividad	Luzmila Zegarra
Secretaría de Gobierno Digital – PCM	Carlos Arias
SUNAT	Jorge Llanos
Consultor	Carlos Horna
Consultor	Gustavo Vallejo

PRÓLOGO
(ISO)

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

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

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no deberán ser responsables de identificar ninguno o todos los derechos de patente. Los detalles de los derechos de patente identificados durante el desarrollo del documento se encontrarán en la Introducción y / o en la lista ISO de declaraciones de patentes recibidas (ver www.iso.org/patents) o IEC lista de declaraciones de patentes recibidas (ver http://patents.iec.ch).

Cualquier nombre comercial utilizado en este documento es información dada para la conveniencia de los usuarios y no constituye un endoso.

Para obtener una explicación sobre la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en las Obstáculos técnicos al comercio (OTC), consulte la siguiente URL: www.iso.org/iso/foreword.html.

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

Esta tercera edición cancela y reemplaza la segunda edición (ISO/IEC 27007:2017), que ha sido revisada técnicamente.

Los principales cambios en comparación con la edición anterior son los siguientes:

- el documento se ha alineado con ISO 19011:2018;
- la Introducción ha sido reformulada y ampliada;
- en 5.1, se ha eliminado todo el texto;
- en 5.2.2, el ítem anterior d) ha sido eliminado;
- en 5.3, se ha eliminado todo el texto;
- en 5.5.2.2, se eliminó el anterior elemento b) y el párrafo siguiente;
- en 6.5.2.2, se eliminó el primer párrafo y se reescribió la Nota.

Cualquier comentario o pregunta sobre este documento debería dirigirse al organismo nacional de normalización del usuario. Puede encontrar una lista completa de estos cuerpos en www.iso.org/members.html.

INTRODUCCIÓN

Se puede conducir una auditoría del sistema de gestión de seguridad de la información (SGSI) en función de una serie de criterios de auditoría, por separado o en combinación, incluyendo, pero no limitado a:

- requisitos definidos en ISO/IEC 27001:2013;
- políticas y requisitos especificados por las partes interesadas relevantes;
- requisitos legales y regulatorios;
- procesos y controles del SGSI definidos por la organización u otras partes;
- planes del sistema de gestión relacionados con la provisión de productos específicos de un SGSI (por ejemplo, planes para abordar los riesgos y oportunidades al establecer el SGSI, planes para lograr objetivos de seguridad de la información, planes de tratamiento de riesgos, planes de proyectos).

Este documento proporciona orientación para todos los tamaños y tipos de organizaciones y auditorías de SGSI de diversos ámbitos y escalas, incluidas las realizadas por grandes equipos de auditoría, generalmente de organizaciones más grandes, y por auditores individuales, ya sea en organizaciones grandes o pequeñas. Esta guía debería adaptarse según corresponda al alcance, la complejidad y la escala del programa de auditoría del SGSI.

Este documento se concentra en las auditorías internas del SGSI (primera parte) y las auditorías del SGSI conducidas por las organizaciones sobre sus proveedores externos y otras partes interesadas externas (segunda parte). Este documento también puede ser útil para las auditorías externas del SGSI conducidas con fines distintos a la certificación por terceros del sistema de gestión de terceros. ISO/IEC 27006 proporciona requisitos para auditar el SGSI por certificadoras de tercera parte; Este documento puede proporcionar una guía adicional útil.

Este documento es para usarse junto con la guía contenida en ISO 19011:2018.

Este documento sigue la estructura de ISO 19011:2018.

ISO 19011:2018 proporciona orientación sobre la gestión de programas de auditoría, la conducción de auditorías internas o externas de los sistemas de gestión, así como sobre la competencia y evaluación de los auditores de sistema de gestión.

El Anexo A proporciona orientación para las prácticas de auditoría del SGSI junto con los requisitos de ISO/IEC 27001:2013, capítulos 4 a 10.

---oooOooo--

Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información

1 Objeto y campo de aplicación

Esta Norma Técnica Peruana proporciona orientación sobre la gestión de un programa de auditoría del sistema de gestión de seguridad de la información (SGSI), sobre la Conduciendo de auditorías y sobre la competencia de los auditores del SGSI, además de la orientación contenida en ISO 19011.

Este Norma Técnica Peruana es aplicable a aquellos que necesitan comprender o conducir auditorías internas o externas de un SGSI o para gestionar un programa de auditoría de SGSI.

2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituya requisitos de esta Norma Técnica Peruana. Para las referencias con fecha, sólo se aplica la edición citada. Para referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO 19011:2018[1]	Directrices para la auditoría de los sistemas de gestión
ISO/IEC 27000:2018	Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario

[1] La norma ISO 19011:2018 es equivalente a la NTP-ISO 19011:2018

3 Términos y definiciones

Para los propósitos de esta Norma Técnica Peruana, se aplican los términos y definiciones dados en ISO 19011 e ISO/IEC 27000.

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

- Plataforma de navegación en línea ISO: disponible en http://www.iso.org/obp .

- IEC Electropedia: disponible en http://www.electropedia.org/.

4 Principios de auditoría

Se aplican los principios de auditoría de ISO 19011:2018, capítulo 4.

5 Gestionar un programa de auditoría

5.1 General

Se aplican las pautas de ISO 19011:2018, 5.1.

5.2 Establecer los objetivos del programa de auditoría

5.2.1 Se aplican las pautas de ISO 19011:2018, 5.2. Además, se aplica la orientación de 5.2.2.

5.2.2 Las consideraciones específicas del SGSI para determinar los objetivos del programa de auditoría1) pueden incluir:

a) requisitos de seguridad de la información identificados;

b) requisitos de ISO/IEC 27001;

c) el nivel de desempeño del auditado, como se refleja en la ocurrencia de eventos e incidentes de seguridad de la información y la efectividad del SGSI;

NOTA: Puede encontrar más información sobre monitoreo, medición, análisis y evaluación del desempeño en ISO/IEC 27004.

d) riesgos de seguridad de la información para las partes relevantes, es decir, el auditado y el cliente de auditoría.

Los ejemplos de objetivos del programa de auditoría específicos del SGSI incluyen:

- demostrar conformidad con todos los requisitos legales y contractuales relevantes y otros requisitos y sus implicaciones de seguridad;
- obtener y mantener la confianza en la capacidad de gestión de riesgos del auditado;
- evaluar la efectividad de las acciones para abordar los riesgos y oportunidades de seguridad de la información.

5.3 Determinar y evaluar los riesgos y oportunidades del programa de auditoría

5.3.1 Se aplican las pautas de ISO 19011:2018, 5.3.

5.3.2 Las medidas para garantizar la seguridad y la confidencialidad de la información deberían determinarse teniendo en cuenta a los auditados y otros requisitos de las partes relevantes. Los requisitos de otras partes pueden incluir requisitos legales y contractuales relevantes.

5.4 Establecer el programa de auditoría

5.4.1 Roles y responsabilidades de las personas que gestionan el programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.4.1. Además, se aplica la guía en 5.4.1.2

5.4.2 Competencia de la persona(s) que gestiona el programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.4.2.

5.4.3 Establecer la extensión del programa de auditoría

5.4.3.1 Se aplican las pautas de ISO 19011:2018, 5.4.3. Además, se aplica la orientación de 5.4.3.2.

5.4.3.2 La extensión de un programa de auditoría puede incluir lo siguiente:

a) el tamaño del SGSI, que incluye:

1) el número total de personas que trabajan bajo el control de la organización y las relaciones con las partes interesadas y los contratistas que son relevantes para el SGSI;

2) el número de sistemas de información;

3) el número de sitios cubiertos por el SGSI;

b) la complejidad del SGSI (incluido el número y la importancia de los procesos y actividades) teniendo en cuenta las diferencias entre los sitios dentro del alcance del SGSI;

c) la importancia de los riesgos de seguridad de la información identificados para el SGSI en relación con el negocio;

d) la importancia de los riesgos y oportunidades determinados al planificar el SGSI;

e) la importancia de preservar la confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI;

f) la complejidad de los sistemas de información a auditar, incluida la complejidad de la tecnología de la información implementada;

g) el número de sitios similares.

Se debería considerar en el programa de auditoría el establecimiento de prioridades que garanticen un examen más detallado basado en la importancia de los riesgos de seguridad de la información y los requisitos comerciales con respecto al alcance del SGSI.

NOTA: Puede encontrar más información sobre la determinación del tiempo de auditoría en ISO/IEC 27006. Puede encontrar más información sobre el muestreo en múltiples sitios en ISO/IEC 27006 y el documento obligatorio 1 del Foro Internacional de Acreditación (IAF MD1, ver Referencia [11]). La información contenida en ISO/IEC 27006 e IAF MD 1 solo se refiere a auditorías de certificación.

5.4.4 Determinar los recursos para el programa de auditoría

5.4.4.1 Se aplican las pautas de ISO 19011:2018, 5.4.4. Además, se aplica la orientación de 5.4.4.2.

5.4.4.2 En particular, para todos los riesgos significativos aplicables al auditado y relevantes para los objetivos del programa de auditoría, a los auditores del SGSI se les debería asignar tiempo suficiente para revisar la efectividad de las acciones para abordar tanto los riesgos de seguridad de la información como los riesgos y oportunidades relacionados con el SGSI.

5.5 Implementación del programa de auditoría

5.5.1 General

Se aplican las pautas de ISO 19011:2018, 5.5.1.

5.5.2 Definición de los objetivos, alcance y criterios para una auditoría individual

5.5.2.1 Se aplican las pautas de ISO 19011:2018, 5.5.2. Además, se aplica la orientación de 5.5.2.2.

5.5.2.2 Los objetivos de la auditoría pueden incluir lo siguiente:

a) evaluación de si el SGSI identifica y aborda adecuadamente los requisitos de seguridad de la información;

b) determinación del grado de conformidad de los controles de seguridad de la información con los requisitos y procedimientos del SGSI.

El alcance de la auditoría debería tener en cuenta los riesgos de seguridad de la información y los riesgos y oportunidades relevantes que afectan el SGSI de las partes relevantes, es decir, el cliente de auditoría y el auditado.

Los siguientes temas pueden considerarse como criterios de auditoría y utilizarse como referencia con respecto a los cuales se determina la conformidad:

a) la política de seguridad de la información, los objetivos de seguridad de la información, las políticas y los procedimientos adoptados por el auditado;

b) requisitos contractuales y otros requisitos relevantes para el auditado;

c) los criterios de riesgo de seguridad de la información del auditado, el proceso de evaluación de riesgos de seguridad de la información y el proceso de tratamiento de riesgos;

d) la Declaración de Aplicabilidad, la identificación de cualquier control específico del sector u otros controles necesarios, la justificación de las inclusiones, si se implementan o no, y la justificación de las exclusiones de los controles de ISO/IEC 27001:2013, Anexo A;

e) la definición de controles para tratar los riesgos adecuadamente;

f) los métodos y criterios para el monitoreo, medición, análisis y evaluación del desempeño de la seguridad de la información y la efectividad del SGSI;

g) requisitos de seguridad de la información proporcionados por el cliente;

h) requisitos de seguridad de la información aplicados por un proveedor o subcontratista.

5.5.3 Seleccionar y determinar los métodos de auditoría

5.5.3.1 Se aplican las pautas de ISO 19011:2018, 5.5.3. Además, se aplica la orientación de 5.5.3.2.

5.5.3.2 Si se realiza una auditoría conjunta, se debería prestar especial atención a la divulgación de información entre las partes relevantes. Se debería llegar a un acuerdo con todas las partes interesadas antes de que comience la auditoría.

5.5.4 Selección de los miembros del equipo auditor

5.5.4.1 Se aplican las pautas de ISO 19011:2018, 5.5.4. Además, se aplica la orientación de 5.5.4.2.

5.5.4.2 La competencia del equipo de auditoría general debería incluir el conocimiento y la comprensión adecuados de:

a) gestión de riesgos de seguridad de la información suficiente para evaluar los métodos utilizados por el auditado;

b) seguridad de la información y gestión de la seguridad de la información suficiente para evaluar la determinación del control, la planificación, la implementación, el mantenimiento y la efectividad del SGSI.

5.5.5 Asignación de la responsabilidad por una auditoría individual al líder del equipo auditor

Se aplican las pautas de ISO 19011:2018, 5.5.5.

5.5.6 Gestión de los resultados del programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.5.6.

5.5.7 Gestión y mantenimiento de los registros del programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.5.7.

5.6 Seguimiento del programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.6.

5.7 Revisión y mejora del programa de auditoría

Se aplican las pautas de ISO 19011:2018, 5.7.

6 Conduciendo una auditoría

6.1 General

Se aplican las pautas de ISO 19011:2018, 6.1.

6.2 Iniciando la auditoría

6.2.1 General

Se aplican las pautas de ISO 19011:2018, 6.2.1.

6.2.2 Establecer el contacto con el auditado

6.2.2.1 Se aplican las pautas de ISO 19011:2018, 6.2.2. Además, se aplica la guía en 6.2.2.2.

6.2.2.2 Cuando sea necesario, se debería tener cuidado para garantizar que los auditores hayan obtenido la autorización de seguridad necesaria para acceder a la información documentada u otra información requerida para las actividades de auditoría (incluida, entre otras, información confidencial o sensitiva).

6.2.3 Determinar la viabilidad de la auditoría

6.2.3.1 Se aplican las pautas de ISO 19011:2018, 6.2.3. Además, se aplica la guía en 6.2.3.2.

6.2.3.2 Antes de que comience la auditoría, se debería preguntar al auditado si existe alguna evidencia de auditoría del SGSI que no está disponible para su revisión por parte del equipo auditor, ejemplo: porque la evidencia contiene información de identificación personal u otra información confidencial / sensible. La persona responsable de Gestionar el programa de auditoría debería determinar si el SGSI puede ser auditado adecuadamente en ausencia de evidencia de auditoría. Si la conclusión es que no es posible auditar adecuadamente el SGSI sin revisar la evidencia de auditoría identificada, la persona responsable de Gestionar el programa de auditoría debería informar al auditado que la auditoría no puede llevarse a cabo hasta que se otorguen los arreglos de acceso apropiados o medios alternativos para lograr la auditoría ha sido propuesta por o por el auditado. Si la auditoría continúa, el plan de auditoría debería tener en cuenta las limitaciones de acceso.

6.3 Preparación de actividades de auditoría

6.3.1 Realizar la revisión de la información documentada

Se aplican las pautas de ISO 19011:2018, 6.3.1.

6.3.2 Planificando la auditoría

6.3.2.1 Se aplican las pautas de ISO 19011:2018, 6.3.2. Además, se aplica la orientación en 6.3.2.2.

6.3.2.2 El líder del equipo auditor debería ser consciente de que la presencia de los miembros del equipo auditor puede generar riesgos para el auditado. La presencia del equipo auditor puede influir en la seguridad de la información y ser una fuente de riesgo adicional para la información del auditado, ejemplo: registros confidenciales o confidenciales o infraestructura del sistema (por ejemplo, borrado accidental, divulgación no autorizada de información, alteración involuntaria de información).

6.3.3 Asignación de trabajo al equipo auditor

Se aplican las pautas de ISO 19011:2018, 6.3.3.

6.3.4 Preparación de información documentada para la auditoría

6.3.4.1 Se aplican las pautas de ISO 19011:2018, 6.3.4. Además, se aplica la orientación en 6.3.4.2.

6.3.4.2 El líder del equipo auditor debería asegurarse de que todos los documentos de trabajo de auditoría se clasifiquen adecuadamente y se manejen de acuerdo con esa clasificación.

6.4 Conduciendo las actividades de auditoría

6.4.1 General

Se aplican las pautas de ISO 19011:2018, 6.4.1.

6.4.2 Asignando roles y responsabilidades de guías y observadores

Se aplican las pautas de ISO 19011:2018, 6.4.2.

6.4.3 Conduciendo la reunión de apertura

Se aplican las pautas de ISO 19011:2018, 6.4.3.

6.4.4 Comunicación durante la auditoría

Se aplican las pautas de ISO 19011:2018, 6.4.4.

6.4.5 Disponibilidad y acceso de información de auditoría

6.4.5.1 Se aplican las pautas de ISO 19011:2018, 6.4.5. Además, se aplica la guía en 6.4.5.2.

6.4.5.2 Si alguna evidencia de auditoría no está disponible para el equipo auditor durante la auditoría por razones de clasificación o sensibilidad, el auditor principal debería determinar en qué medida esto afecta la confianza en los hallazgos y conclusiones de la auditoría, y reflexionar sobre ello en el informe de auditoría sin comprometer la sensibilidad de la evidencia que no estaba disponible.

6.4.6 Revisión de la información documentada mientras se conduce la auditoría

6.4.6.1 Se aplican las pautas de ISO 19011:2018, 6.4.6. Además, se aplica la guía en 6.4.6.2.

6.4.6.2 Los auditores del SGSI deberían verificar que la información documentada según lo requerido por los criterios de auditoría y relevante para el alcance de la auditoría exista y se ajuste a los requisitos de los criterios de auditoría.

Los auditores del SGSI deberían confirmar que los controles determinados dentro del alcance de la auditoría están relacionados con los resultados de la evaluación de riesgos y el proceso de tratamiento de riesgos, y posteriormente pueden rastrearse hasta la política y los objetivos de seguridad de la información.

NOTA: El Anexo A proporciona orientación para la práctica de auditoría del SGSI, incluido cómo auditar el SGSI utilizando información documentada relevante.

6.4.7 Recopilar y verificar información

6.4.7.1 Se aplican las pautas de ISO 19011:2018, 6.4.7. Además, se aplica la guía en 6.4.7.2.

6.4.7.2 Los posibles métodos para recopilar información relevante durante la auditoría incluyen:

a) revisión de información documentada (incluyendo registros de computadora y datos de configuración);

b) visita a las instalaciones de procesamiento de información;

c) observación de los procesos del SGSI y los controles relacionados;

d) uso de herramientas de auditoría automatizadas.

NOTA 1: El Anexo A proporciona orientación sobre cómo auditar los procesos del SGSI.

NOTA 2: ISO/IEC TS 27008 proporciona orientación adicional sobre cómo evaluar los controles de seguridad de la información.

Los miembros del equipo de auditoría del SGSI debería garantizar el manejo adecuado de toda la información recibida de los auditados de acuerdo con el convenio entre el cliente de auditoría, el equipo de auditoría y el auditado.

6.4.8 Generando hallazgos de auditoría

Se aplican las pautas de ISO 19011:2018, 6.4.8.

6.4.9 Determinando las conclusiones de auditoría

Se aplican las pautas de ISO 19011:2018, 6.4.9.

6.4.10 Conducir la reunión de cierre

Se aplican las pautas de ISO 19011:2018, 6.4.10.

6.5 Preparación y distribución del informe de auditoría.

6.5.1 Preparación del informe de auditoría

Se aplican las pautas de ISO 19011:2018, 6.5.1.

6.5.2 Distribuir el informe de auditoría

6.5.2.1 Se aplican las pautas de ISO 19011:2018, 6.5.2. Además, se aplica la guía en 6.5.2.2.

6.5.2.2 Nota

Nota: Al utilizar medios electrónicos para la distribución del informe de auditoría, una apropiada encriptación es una posible medida para garantizar los requisitos de confidencialidad.

6.6 Completando la auditoría

Se aplican las pautas de ISO 19011:2018, 6.6.

6.7 Conducir la auditoría de seguimiento

Se aplican las pautas de ISO 19011:2018, 6.7.

7 Competencia y evaluación de los auditores

7.1 General

Se aplican las pautas de ISO 19011:2018, 7.1.

7.2 Determinación de la competencia del auditor

7.2.1 General

7.2.1.1 Se aplican las pautas de ISO 19011:2018, 7.2.1. Además, se aplica la guía en 7.2.1.2.

7.2.1.2 Al decidir el conocimiento y las habilidades apropiadas de un auditor de SGSI, se debería tener en cuenta lo siguiente:

a) complejidad del SGSI (por ejemplo, criticidad de los sistemas de información dentro del SGSI, resultados de la evaluación de riesgos del SGSI);

b) los tipos de negocios incluidos dentro del alcance del SGSI;

c) extensión y diversidad de la tecnología utilizada en la implementación de los diversos componentes del SGSI (tales como los controles implementados, información documentada y / o control de procesos, plataformas tecnológicas y soluciones involucradas, entre otros.);

d) rendimiento previamente demostrado del SGSI;

e) alcance de la contratación externa y arreglos de terceros externos utilizados dentro del alcance del SGSI;

f) las normas, requisitos legales y otros requisitos relevantes para el programa de auditoría.

7.2.2 Comportamiento personal

Se aplican las pautas de ISO 19011:2018, 7.2.2.

7.2.3 Conocimientos y habilidades

7.2.3.1 General

Se aplican las pautas de ISO 19011:2018, 7.2.3.1.

7.2.3.2 Conocimientos genéricos y habilidades de los auditores del sistema de gestión.

Se aplican las pautas de ISO 19011:2018, 7.2.3.2.

7.2.3.3 Disciplina y competencia sectorial específica de los auditores

7.2.3.3.1 Se aplican las pautas de ISO 19011:2018, 7.2.3.3. Además, se aplica la guía en 7.2.3.3.2.

7.2.3.3.2 Los auditores del SGSI también deberían poder comprender los requisitos comerciales relevantes.

7.2.3.4 Competencia genérica del líder del equipo auditor

Se aplican las pautas de ISO 19011:2018, 7.2.3.4.

7.2.3.5 Conocimientos y habilidades para auditar múltiples disciplinas.

Se aplican las pautas de ISO 19011:2018, 7.2.3.5.

7.2.4 Alcanzar la competencia del auditor

7.2.4.1 Se aplican las pautas de ISO 19011:2018, 7.2.4. Además, se aplica la guía en 7.2.4.2.

7.2.4.2 Los auditores del SGSI deberían tener conocimientos y habilidades en tecnología de la información y seguridad de la información, demostrados por ejemplo a través de certificaciones relevantes (por ejemplo, acreditadas según ISO/IEC 17024). La experiencia laboral individual de los auditores del SGSI también debería contribuir al desarrollo de sus conocimientos y habilidades en el campo del SGSI.

NOTA: Puede encontrar más información sobre la certificación para auditores de SGSI en ISO/IEC 27006.

7.2.5 Alcanzar la competencia líder del equipo auditor

Se aplican las pautas de ISO 19011:2018, 7.2.5.

7.3 Estableciendo los criterios de evaluación del auditor

Se aplican las pautas de ISO 19011:2018, 7.3.

7.4 Seleccionar el método apropiado de evaluación de auditor

Se aplican las pautas de ISO 19011:2018, 7.4.

7.5 Conduciendo la evaluación del auditor

Se aplican las pautas de ISO 19011:2018, 7.5.

7.6 Mantener y mejorar de la competencia del auditor

Se aplican las pautas de ISO 19011:2018, 7.6.

ANEXO A
(INFORMATIVO)

Orientación para la práctica de auditoría del SGSI

A.1 Descripción general

Este anexo proporciona una guía genérica sobre cómo auditar un SGSI, para lo cual una organización afirma que cumple con ISO/IEC 27001. Como esta guía está destinada a aplicarse a todas las auditorías de dicho SGSI, independientemente del tamaño o la naturaleza de la organización involucrada, esta guía es genérica. La guía está destinada a ser utilizada por auditores que realicen auditorías de SGSI, ya sean internas o externas.

NOTA: ISO/IEC 27003 proporciona orientación sobre la implementación y operación de un SGSI de acuerdo con ISO/IEC 27001.

A.2 General

A.2.1 Objetivos de auditoría, alcance, criterios y evidencia de auditoría

Durante las actividades de auditoría, la información relevante para los objetivos, el alcance y los criterios de la auditoría, incluida la información relacionada con las interfaces entre funciones, actividades y procesos, debería obtenerse mediante un muestreo apropiado y debería verificarse. Solo la información verificable debería aceptarse como evidencia de auditoría. La evidencia de auditoría que conduce a los resultados de la auditoría debería ser registrada.

Los métodos para obtener información incluyen los siguientes:

- entrevistas;
- observaciones;
- revisión de documentos, incluidos los registros.

A.2.2 Estrategia para auditar un SGSI

Existen algunas subcapítulos de la ISO/IEC 27001:2013 que están estrechamente relacionadas y que, en la práctica, a menudo se tratan mejor en el mismo tiempo al realizar la auditoría. Consulte la Tabla A.2 para ver ejemplos.

Los ejemplos en ISO/IEC 27001:2013 son 6.1.3, 8.3 y 6.2, 5.1, 5.2, 5.3, 7.1, 7.4, 7.5, 9.1, 9.3 y 10.2 y tiene sentido auditar estos subcapítulos con los subcapítulos vinculados y relacionados.

ISO/IEC 27001:2013, 7.5 presenta los requisitos relativos a la información documentada. Como se explica en la Tabla A.2, A.4.5, cada vez que los auditores examinan un elemento de información documentada, ofrece la oportunidad de confirmar la conformidad con los requisitos de ISO/IEC 27001:2013, 7.5. La guía sobre cómo hacer esto se encuentra en la Tabla A.2, A.4.5. Los requisitos con respecto a la información documentada no se repiten para cada aparición de "información documentada " en la tabla.

A.2.3 Auditoría e información documentada

Las actividades de auditoría pueden involucrar información documentada, a saber:

a) las declaraciones de requisitos de información documentada en ISO/IEC 27001 pueden usarse como criterios de auditoría;

b) información documentada requerida por ISO/IEC 27001:2013, 7.5.1 b);

c) información documentada determinada por la organización como necesaria para la efectividad del SGSI de ISO/IEC 27001:2013, 7.5.1 c).

Puede haber evidencia de auditoría que no sea A.2.3 b), que los auditores obtendrán a través de entrevistas, observaciones y revisión de documentos, incluidos los registros.

Se puede encontrar una discusión detallada de la información documentada sobre ISO/IEC 27001 en A.3.

A.3 Orientación sobre los requisitos de información documentada en ISO/IEC 27001

A.3.1 Razonamiento

Los auditores deberían tener cuidado al solicitar información documentada como evidencia de conformidad.

Así tenemos:

a) 16 requisitos explícitos para la información documentada, incluida la Declaración de Aplicabilidad, tal como se detalla en la Tabla A.1;

b) los requisitos restantes son requisitos para los cuales:

1) sería razonable esperar que la evidencia de la conformidad se pueda encontrar en la mencionada información documentada;

2) no existe un requisito explícito o implícito de información documentada.

Tabla A.1 - Requisitos para la información documentada en ISO/IEC 27001

Requisito de información documentada sobre	Referencia en ISO/IEC 27001:2013
Alcance del SGSI	4.3
Política de seguridad de la información	5.2
Proceso de evaluación de riesgos de seguridad de la información	6.1.2
Proceso de tratamiento de riesgos de seguridad de la información	6.1.3
Declaración de aplicabilidad	6.1.3 d)
Objetivos de seguridad de la información	6.2
Evidencia de competencia	7.2 d)
Información documentada determinada por la organización como necesaria para la efectividad del SGSI	7.5.1 b)
Planificación y control operacional	8.1
Resultados de las evaluaciones de riesgos de seguridad de la información	8.2
Resultados del tratamiento de riesgos de seguridad de la	8.3
información	

Requisito de información documentada sobre	Referencia en ISO/IEC 27001:2013
Evidencia de los resultados de monitoreo y medición	9.1
Evidencia de los programas de auditoría y los resultados de la auditoría	9.2 g)
Evidencia de los resultados de las revisiones de la gerencia	9.3
Evidencia de la naturaleza de las no conformidades y cualquier acción posterior tomada	10,1 f)
Evidencia de los resultados de cualquier acción correctiva	10,1 g)

NOTA: La definición de una auditoría establece que es un proceso documentado y, por lo tanto, un auditor puede esperar que el requisito de ISO/IEC 27001:2013, 9.2 resulte en un proceso de auditoría documentada.

A.3.2 Ejemplo de requisito implícito de información documentada

Como ejemplo de A.3.1 b) 1), considere ISO/IEC 27001:2013, 6.1.2, que requiere que las organizaciones "retengan información documentada sobre el proceso de evaluación de riesgos de seguridad de la información". Los requisitos anteriores [ISO/IEC 27001:2013, 6.1.2 a) al e)] se refieren a ese proceso de evaluación de riesgos. Por lo tanto, es razonable esperar que se encuentre evidencia de conformidad con estos requisitos en la información documentada requerida sobre el proceso de evaluación de riesgos.

A.3.3 Ejemplo donde no existe un requisito explícito o implícito de información documentada

Como ejemplo de A.3.1 b) 2), considere ISO/IEC 27001:2013, 4.1.1. No se requiere información documentada sobre asuntos externos e internos. Por lo tanto, los auditores no deberían exigir verlo. Sin embargo, el hecho de que la organización no demuestre que ha determinado estos problemas constituiría una no conformidad con ISO/IEC 27001:2013, 4.1.1. Sin embargo, la responsabilidad recae en la organización para determinar cómo elige demostrar conformidad. Puede ser que la alta gerencia pueda explicarlo (es decir, alguien lo sabe); puede ser que haya actas de una reunión en la que se discutió el tema; se puede evidenciar en información documentada que se encuentra bajo gestión de configuración formal o se puede evidenciar de alguna otra manera. De hecho, es probable que la evidencia se distribuya entre la información documentada del SGSI. Por ejemplo, el propósito de ISO/IEC 27001:2013, 4.1.1, es ayudar a la organización a comprender el contexto de su SGSI. Ese contexto prevalece en todo el SGSI, particularmente en la determinación del alcance y la política y en el desempeño de los procesos de evaluación y tratamiento de

riesgos. Si la organización ha cumplido los requisitos de ISO/IEC 27001:2013, 4.1.1, es probable que su conocimiento de los problemas externos e internos se utilice en estas otras áreas del SGSI, su uso será coherente y probablemente habrá evidencia de conformidad en la información documentada sobre estas otras áreas.

A.4 La declaración de aplicabilidad

La Declaración de Aplicabilidad (SOA) es otra área que requiere atención. El SOA debería contener todos los controles necesarios, es decir, los controles que la organización tiene, como resultado de su proceso de tratamiento de riesgos [ISO/IEC 27001:2013, 6.1.3 c)], determinado como necesario para la modificación del riesgo de seguridad de la información para cumplir con sus criterios de aceptación de riesgos. Todos los controles necesarios son los requisitos propios de la organización.

Los controles necesarios pueden ser ISO/IEC 27001:2013, Anexo A, controles, pero no son obligatorios. Pueden ser controles tomados de otras normas (por ejemplo, ISO/IEC 27017) u otras fuentes, o pueden haber sido diseñados especialmente por la organización.

En algunos casos, la organización utiliza un control que es una variación de un control ISO/IEC 27001:2013, Anexo A, y excluye el control original ISO/IEC 27001:2013, Anexo A, el control, la razón para la exclusión es que tiene sido por reemplazado por la variación del control de la organización. Alternativamente, la variación puede incorporar el control ISO/IEC 27001:2013, Anexo A, y, por lo tanto, no estaría excluido.

Los auditores deberían buscar la conformidad con la especificación de la organización de sus controles necesarios, no con la especificación dada en ISO/IEC 27001:2013, Anexo A. Si la especificación de la organización requiere un procedimiento documentado, entonces esto forma parte de la conformidad de la organización con ISO/IEC 27001:2013, 7.5.1 b). Si no es así, los auditores no deberían exigir verlo. Sin embargo, los auditores deberían tener en cuenta el requisito [ISO/IEC 27001:2013, 8.1)] de que la organización debería "mantener la información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo previsto". Desde ISO/IEC 27001:2013, 8.1 se refiere a ISO/IEC 27001:2013, 6.1, el plan de tratamiento de riesgos de la organización y, por lo tanto, sus controles necesarios, están dentro del alcance de este requisito de información documentada.

Al auditar la selección de controles, es mejor auditar contra los planes de tratamiento de riesgos de seguridad de la información [como se establece en ISO/IEC 27001:2013, 6.1.3 e)] en lugar de los controles individuales necesarios como se enumeran en la Declaración de aplicabilidad. Esto se debería a que los planes de tratamiento de riesgos de seguridad de la información probablemente especifiquen la interacción entre los controles necesarios, lo cual es una consideración que puede perderse si solo se utilizó la Declaración de Aplicabilidad.

A.5 Otra información documentada

El enfoque de ISO/IEC 27001 está en los resultados. De los 16 requisitos explícitos para la información documentada (ver Tabla A.1), solo tres se refieren a especificaciones (el proceso de evaluación de riesgos de seguridad de la información, el proceso de tratamiento de riesgos de seguridad de la información y el programa de auditoría). Sin embargo, esto no impide que una organización tenga procedimientos documentados. Dicha documentación de respaldo cae dentro del alcance de ISO/IEC 27001:2013, 7.5.1 b) (información documentada determinada por la organización como necesaria para la efectividad de su SGSI). Por lo tanto, se convierte en un requisito de una organización y, como tal, debería estar dentro del alcance de una auditoría.

A.6 Notas

La información requerida puede ser parte de una página web o presentarse al lector como el resultado de una consulta a la base de datos. Además, con la excepción de la Declaración de Aplicabilidad, ISO/IEC 27001 no da nombres a los documentos. Por lo tanto, es posible que la información documentada sobre la política de seguridad de la información no se encuentre en un documento o página web llamada "Política de seguridad de la información". Las organizaciones tienen derecho a llamar a la política de seguridad de la información otra cosa. Las personas con la responsabilidad y autoridad para garantizar que el sistema de gestión de seguridad de la información cumpla con los requisitos de ISO/IEC 27001:2013, 5.3 a), sean los mismos, deberían conocer la relación entre los requisitos de información documentada exigidos por ISO/IEC 27001 y su información documentada.

A.7 Orientación para auditar un SGSI

La Tabla A.2 enumera la siguiente información:

- primera fila: el número y el nombre del subcapítulo correspondiente de la ISO/IEC 27001:2013;
- segunda fila: capítulos relacionados (consulte A.2.2 para obtener información sobre cómo utilizar esta fila);
- tercera fila: definiciones relevantes de ISO/IEC 27000:2018 para el subcapítulo correspondiente de la ISO/IEC 27001:2013;
- cuarta fila: "Evidencia de auditoría" posibles fuentes de información sobre el subcapítulo correspondiente de la ISO/IEC 27001:2013;
- quinta fila: "Guía práctica de auditoría" guía para la auditoría (consulte A.3);
- sexta fila: "Documentos de apoyo" referencia a otros documentos que pueden ser útiles para la auditoría según el subcapítulo correspondiente de la ISO/IEC 27001:2013.

Tabla A.2 – Directrices de auditoría para ISO/IEC 27001

A.1. Contexto de la organización (ISO/IEC 27001:2013, Capítulo 4)	
A.1.1 Comprender la organización y su contexto ((ISO/IEC 27001:2013, 4.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 6.1, 9.3
Definiciones relevantes ISO/IEC 27000	Contexto externo, seguridad de la información, contexto interno, sistema de gestión, organización
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) los problemas importantes que pueden afectar, ya sea positiva o negativamente, el SGSI; b) la organización;

	c) el propósito de la organización; d) el resultado previsto del SGSI. Las posibles fuentes de los problemas importantes pueden incluir: a) características o condiciones ambientales relacionadas con el clima, la contaminación, la disponibilidad de recursos y la biodiversidad, y el efecto que estas condiciones pueden tener en la capacidad de la organización para alcanzar sus objetivos; b) el contexto externo cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, ya sea internacional, nacional, regional o local; c) características o condiciones de la organización, tales como el gobierno organizacional, los flujos de información y los procesos de toma de decisiones; - políticas organizacionales, objetivos y las estrategias que existen para lograrlos; - la cultura de la organización; - normas, directrices y modelos adoptados por la organización; - el ciclo de vida de los productos y servicios de la organización; - sistemas de información, procesos, ciencia y tecnología subyacentes a la gestión de la seguridad de la información; d) tendencias de auditorías y evaluación de riesgos.
Guía práctica de auditoría	Los auditores deberían confirmar que la organización: a) tiene una comprensión de alto nivel (por ejemplo, estratégica) de los problemas importantes que pueden afectar, ya sea positiva o negativamente, el SGSI; b) conoce los problemas externos e internos que son relevantes para su propósito y que afectan su capacidad para lograr los resultados previstos de su SGSI.

	NOTA 1: El requisito en ISO/IEC 27001:2013 4.3 es "considerar los problemas externos e internos mencionados en ISO/IEC 27001:2013 4.1". Una organización puede tener en cuenta algo que no necesariamente aparece en el resultado. Los auditores también deberían confirmar que los resultados previstos incluyen la preservación de la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y que los riesgos se gestionan adecuadamente. Los auditores también deberían verificar que los temas incluyan temas importantes para la organización, problemas para debate y discusión, o circunstancias cambiantes y también deberían verificar que el conocimiento adquirido se utiliza para guiar los esfuerzos de la organización para planificar, implementar y operar la gestión sistema.
Documentos de respaldo	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.1
A.1.2 Comprender las necesidades y expectativas de las partes interesadas (ISO/IEC 27001:2013, 4.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.1, 4.3
Definiciones Relevantes de ISO/IEC 27000	Parte interesada
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) las partes interesadas; b) las necesidades y expectativas de las partes interesadas relevantes que sean aplicables al SGSI e ISO/IEC 27001. NOTA 2: Las posibles partes interesadas pueden incluir: a) autoridades legales y reguladoras (locales, regionales, estatales / provinciales, nacionales o internacionales); b) organizaciones de padres; c) clientes; d) asociaciones comerciales y profesionales; e) grupos comunitarios; f) organizaciones no gubernamentales;

	g) proveedores; h) vecinos; i) miembros de la organización y otros que trabajan en nombre de la organización; j) expertos en seguridad de la información. NOTA 3 Los requisitos de las partes interesadas pueden incluir: a) leyes; b) permisos, licencias u otras formas de autorización; c) órdenes emitidas por agencias reguladoras; d) sentencias de tribunales o tribunales gestionativos; e) tratados, convenciones y protocolos; f) códigos y estándares industriales relevantes; g) contratos que se han celebrado; h) acuerdos con grupos comunitarios u organizaciones no gubernamentales; i) acuerdos con autoridades públicas y clientes; j) requisitos organizativos; k) principios voluntarios o códigos de práctica; l) etiquetado voluntario o compromisos medioambientales; m) obligaciones derivadas de acuerdos contractuales con la organización; n) intercambio de información y comunicación. NOTA 4: Las partes interesadas pueden tener intereses diferentes, que pueden estar totalmente alineados, parcialmente alineados u opuestos a los objetivos comerciales de la organización. Un ejemplo de dónde una parte interesada tiene intereses opuestos a los objetivos de la organización es el hacker. El hacker requiere que la organización tenga una seguridad débil. La organización debería tener en cuenta este requisito de parte interesada al tener todo lo contrario, es decir, una fuerte seguridad. Los auditores deberían ser conscientes de que el SGSI considera todas las fuentes de riesgo internas y externas. Por lo tanto, la comprensión de la organización de las partes interesadas que se oponen a la organización y sus requisitos es muy relevante.

Guía práctica de auditoría	Los auditores deberían confirmar que la organización tiene una comprensión de alto nivel (por ejemplo, estratégica) de las necesidades y expectativas de las partes interesadas relevantes que son aplicables al SGSI e ISO/IEC 27001. Los auditores deberían verificar que la organización haya identificado los requisitos de la parte interesada que decide adoptar o celebrar voluntariamente un acuerdo o contrato, así como las necesidades y expectativas que son obligatorias porque han sido incorporadas a las leyes, reglamentos y permisos. y licencias por acción gubernamental o judicial. Se observa que no todos los requisitos de las partes interesadas son requisitos de la organización y algunos no son aplicables a la organización o relevantes para el SGSI. Algunas necesidades de las partes interesadas (por ejemplo, las de un pirata informático) serán contrarias al propósito del SGSI y se esperaría que la organización garantice mediante controles de seguridad de la información adecuados que tales necesidades y expectativas no se satisfacen. Los auditores pueden también confirman que hay partes interesadas que se perciben a ser afectados por el SGSI y de ser así, lo comunican a la organización. Los auditores también pueden verificar que la organización utiliza el conocimiento adquirido para guiar sus esfuerzos para planificar, implementar y operar el SGSI.
Documentos de respaldo	ISO 31000:2009, 5.3 ISO/IEC 27003:2017, 4.2
A.1.3 Determinación del alcance del sistema de gestión de seguridad de la información (ISO/IEC 27001:2013, 4.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.1, 4.2
Definiciones relevantes de ISO/IEC 27000	Subcontratar
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información de: - el alcance del sistema de gestión de la organización (según lo definido por ISO/IEC 27001:2013, 4.3); - el alcance de la certificación de una organización, si corresponde; - la Declaración de Aplicabilidad.

	NOTA 5: El alcance de la certificación de una organización no es necesariamente el mismo que el alcance de su ISMS. En general, el alcance de la certificación se limitará a la organización del SGSI.
Guía práctica de auditoría	Los auditores deberían confirmar que la organización establece los límites físicos, informativos, legales y organizativos a los que se aplica el SGSI, a su propia voluntad y elige implementar ISO/IEC 27001 dentro de toda la organización o como una unidad específica o funciones particulares dentro de una organización. Los auditores deberían verificar la comprensión de la organización de su contexto (ISO 27001:2013, 4.1), los requisitos de las partes interesadas relevantes (ISO 27001:2013, 4.2) y las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones [ISO 27001:2013, 4.3 c)], han sido adecuadamente considerado al establecer el alcance del SGSI. Los auditores deberían confirmar además que la evaluación de riesgos de seguridad de la información y el tratamiento de riesgos de la organización reflejan adecuadamente sus actividades y se extienden a los límites de sus actividades tal como se definen en el alcance del SGSI, en la medida aplicable al alcance de la auditoría. Los auditores deberían verificar que haya al menos una Declaración de aplicabilidad por alcance y que todos los controles determinados en el proceso de gestión de riesgos estén incluidos en la (s) Declaración (es) de Aplicabilidad. Estos controles son los controles necesarios a los que se hace referencia en ISO/IEC 27001:2013, 6.1.3 b) y no son necesariamente controles ISO/IEC 27001:2013, Anexo A controles. Pueden incluir controles específicos del sector y controles diseñados por la organización o identificados desde cualquier fuente. Los auditores también deberían confirmar que las interfaces con servicios o actividades que no están completamente dentro del alcance del SGSI se abordan dentro del SGSI sujeto a auditoría y se incluyen en la evaluación de riesgos de seguridad de la información de la organización. Un ejemplo de tal situación es el intercambio de instalaciones (por ejemplo, sistemas de TI, bases de datos y sistemas de telecomunicaciones o la externalización de una función comercial) con otras organizaciones. Debería verificarse que la documentación del alcance se crea y controla de acuerdo con los requisitos de información documentada (ISO/IEC 27001:2013, 7.5).

Documentos de respaldo	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.3 ISO/IEC 27006:2015, 8.2, 9.1.3.5 ISO/IEC 17021-1:2015, 8.2.2
A.1.4 Sistema de gestión de seguridad de la información (ISO/IEC 27001:2013, 4.4)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 6.1.1, 6.1.2, 6.1.3, 8.1, 8.2, 8.3
Definiciones ISO/IEC 27000 relevantes	Mejora continua, seguridad de la información, sistema de gestión.
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre los procesos que deberían establecerse en ISO/IEC 27001, que incluyen: a) procesos para el sistema de gestión (ISO/IEC 27001:2013, 4.4); b) procesos de planificación y control operativo, incluidos los procesos tercerizados (ISO/IEC 27001:2013, 8.1); c) procesos para abordar riesgos y oportunidades al planificar el SGSI, incluido los procesos de evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.2 y / o 8.1.2) y los procesos de tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013,6.1.3 y / u 8.1.3); d) procesos para lograr objetivos de seguridad de la información.
Guía práctica de auditoría	Los auditores deberían confirmar que la organización crea lo "necesario pero suficiente" conjunto de procesos y controles que, juntos, forman un sistema de gestión eficaz en conformidad con ISO/IEC 27001 y establece el SGSI del conjunto de aquellos interrelacionados o elementos interactuantes. Los auditores también deberían confirmar que la organización, en su capacidad actual, conserva autoridad, responsabilidad y autonomía para decidir cómo cumplirá el SGSI requisitos, incluido el nivel de detalle y el grado en que integrará el SGSI requisitos en su negocio.
Documentos de soporte	ISO 31000:2018, 5.3 ISO/IEC 27003:2017, 4.4
A.2 Liderazgo (ISO/IEC 27001:2013, Clausula 5)	
A.2.1 Liderazgo y compromiso (ISO/IEC 27001:2013, 5.1)	
Subcapítulos	ISO/IEC 27001:2013, 4.1, 4.2, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.1, 7.4, 8.1, 9.3, 10.2

ISO/IEC 27001 relacionadas	
Definiciones ISO/IEC 27000 relevantes	Seguridad de la información, alta dirección
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) la política de seguridad de la información [ISO/IEC 27001:2013, 5.1 a)]; b) los objetivos de seguridad de la información [5.1 a)]; c) los procesos de la organización; d) resultados de las revisiones de gestión [5.1 c), e) y g)]; e) evaluación de la necesidad de recursos; f) comunicación de la importancia de una gestión eficaz de la seguridad de la información y de ajustarse a los requisitos del sistema de gestión de la seguridad de la información. También se puede obtener evidencia a través de entrevistas con la alta gerencia. Los resultados de las revisiones de la gestionación también pueden proporcionar evidencia de auditoría con subcapítulos distintas de 5.1 c), e) y g).
Guía práctica de auditoría	Los auditores deberían confirmar el apoyo visible, la participación y el compromiso de la alta dirección de la organización, lo cual es importante para la implementación exitosa de ISO/IEC 27001. Los auditores también deberían verificar que: a) se identifican las tareas delegadas de la alta dirección; b) la alta dirección sigue siendo responsable de la finalización satisfactoria de las actividades asignadas a la organización; c) la alta gerencia asegura que la política y los objetivos de seguridad de la información se establecen y están alineados con la dirección estratégica de la organización general; d) la alta dirección comunica la importancia de una gestión eficaz de la seguridad de la información y de cumplir con los requisitos del SGSI;

	e) la alta dirección se asegura de que el SGSI logre el (los) resultado (s) previsto (s) al apoyar la implementación de todos los procesos de gestión de seguridad de la información y, en particular, mediante la solicitud y revisión de informes sobre el estado y la eficacia del SGSI [véase ISO/IEC 27001:2013, 5.3 b)]; f) la alta dirección dirige y apoya a las personas de la organización directamente involucradas con la seguridad de la información y el SGSI; g) la alta dirección asegura la integración de los requisitos del SGSI en los procesos de la organización; h) la alta gerencia asegura la disponibilidad de recursos para tener un SGSI efectivo; i) la alta gerencia evalúa las necesidades de recursos durante las revisiones de la gerencia y establece objetivos para la mejora continua y para monitorear la efectividad de las actividades planificadas; j) la alta dirección crea una cultura y un entorno que alienta a las personas a trabajar activamente para implementar los requisitos del SGSI y tratar de alcanzar los objetivos de seguridad de la información.
Documentos de soporte	ISO 31000:2018, 4.2 ISO/IEC 27003:2017, 5.1
A.2.2 Política (ISO/IEC 27001:2013, 5.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 6.2, 7.4
Definiciones ISO/IEC 27000 relevantes	Seguridad de la información, política
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) política de seguridad de la información (5.1); b) objetivos de seguridad de la información [ISO/IEC 27001:2013, 5.2 b) y ISO/IEC 27001:2013, 6.2].

Guía práctica de auditoría	Los auditores deberían confirmar que: a) la política de seguridad de la información específica los compromisos organizativos de alto nivel requeridos por ISO/IEC 27001, teniendo en cuenta el propósito de la organización; b) la política de seguridad de la información se utiliza para enmarcar o construir los objetivos de seguridad de la información que la organización establece para sí misma, o se establece explícitamente como parte de la política de seguridad de la información; c) la información documentada de la política de seguridad de la información se crea y controla de acuerdo con los requisitos de la información documentada (7.5); d) la política de seguridad de la información se comunica internamente, de conformidad con los requisitos del subcapítulo de comunicación (7.4); e) la política de seguridad de la información también se pone a disposición de otras partes interesadas, según corresponda. Con la política de seguridad de la información que contiene un compromiso para satisfacer requisitos, en particular, leyes y reglamentos pertinentes, el SGSI no debería ser desestimado de conformidad siempre que resulte en la detección rápida y la acción correctiva de las deficiencias del sistema que contribuyeron a la (s) instancia (s) de no conformidad.
Documentos de soporte	ISO 31000:2018, 4.3.2 ISO/IEC 27003:2017, 5.2
A.2.3 Roles organizativos, responsabilidades y autoridades (ISO/IEC 27001:2013, 5.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 7.4, 9.2, 9.3
Definiciones relevantes de ISO/IEC 27000	Seguridad de la información, organización, alta dirección.
Evidencia de auditoría	Considerando ISO/IEC 27001:2013, 7.5.1 b), la evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) los roles organizacionales;

	b) la descripción del trabajo de las personas que realizan trabajos bajo su control que pueden tener un impacto en el desempeño de la seguridad de la información de la organización; c) la implementación del programa de auditoría interna y los resultados de la auditoría; d) el alcance y la estructura del SGSI de la organización. Además, puede haber más evidencia de auditoría obtenida a través de información documentada u otra información sobre los resultados de las revisiones de la gerencia.
Guía práctica de auditoría	Los auditores deberían confirmar mediante la revisión de información documentada y/o entrevista que: a) las responsabilidades y autoridades para la implementación de los requisitos del SGSI se asignan a roles relevantes dentro de la organización; b) la alta dirección es responsable de estas responsabilidades y las autoridades se asignan y comunican a las personas respectivas que desempeñan esas funciones; c) las responsabilidades y autoridades se comunican de acuerdo con los requisitos del subcapítulo de comunicación (ISO/IEC 27001:2013, 7.4); d) la demostración de conformidad con los requisitos de ISO/IEC 27001 se realiza de acuerdo con los requisitos de la auditoría interna (ISO/IEC 27001:2013, 9.2); e) los informes de rendimiento se realizan de acuerdo con los requisitos de la revisión de gestión (ISO/IEC 27001:2013, 9.3); Los auditores deberían verificar que las personas responsables tengan acceso suficiente a la alta gerencia para mantener a la gerencia informada sobre el estado y el desempeño del SGSI. NOTA 6: La función de garantizar que el sistema de gestión cumpla con los requisitos de ISO/IEC 27001 puede asignarse a un individuo, compartirse por varios individuos o asignarse a un equipo.
Documentos de respaldo	ISO 31000:2018, 4.3.3 ISO/IEC 27003:2017, 5.3

A.3 Planificación (ISO/IEC 27001:2013, clausula 6)	
A.3.1 Acciones para abordar riesgos y oportunidades (ISO/IEC 27001:2013, 6.1)	
A.3.1.1 General (ISO/IEC 27001:2013, 6.1.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.1, 4.2, 8.1, 9, 10.2
Definiciones relevantes de ISO/IEC 27000	Seguridad de la información, riesgo, gestión del riesgo
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) planificación del SGSI [ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) y 8.1)]; b) el proceso de evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.2); c) los resultados de las evaluaciones de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.2); d) el proceso de tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.3); e) los resultados del tratamiento del riesgo de seguridad de la información (ISO/IEC 27001:2013, 8.3); f) los resultados del monitoreo y las mediciones (9.1); (ISO/IEC 27001:2013, 9.1); g) el programa o programas de auditoría interna y los resultados de la auditoría interna (ISO/IEC 27001:2013, 9.2); h) los resultados de las revisiones de gestión (ISO/IEC 27001:2013, 9.3); i) contexto de la organización (ISO/IEC 27001:2013, 4); j) objetivos de seguridad de la información (ISO/IEC 27001:2013, 6.2).
Guía práctica de auditoría	Los auditores deberían confirmar que la planificación: a) se realiza a un nivel apropiado para establecer el SGSI;

	b) incluye la consideración de los asuntos relevantes para el contexto de la organización identificado en (ISO/IEC 27001:2013, 4.1) y los requisitos aplicables de la organización identificados en (ISO/IEC 27001:2013, 4.3) para abordar cualquier consecuencia negativa o positiva relacionada con ISO/IEC 27001:2013, 6.1.1 a) a c); c) ha anticipado posibles escenarios y consecuencias y, como tal, es preventivo para abordar los efectos no deseados antes de que ocurran; d) aborda los resultados previstos [ISO/IEC 27001:2013, 6.1.1 a)] determinados por la organización que incluyen preservar la confidencialidad, integridad y disponibilidad de información mediante la aplicación de un proceso de gestión de riesgos; e) incluye determinar cómo incorporar las acciones que se consideran necesarias o beneficiosas en el SGSI, ya sea a través del establecimiento de objetivos (ISO/IEC 27001:2013, 6.2), el control operativo (ISO/IEC 27001:2013, 8.1) u otros subcapítulos específicos de ISO/IEC 27001, por ejemplo, disposiciones de recursos (ISO/IEC 27001:2013, 7.1), competencia (ISO/IEC 27001:2013, 7.2), evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.2), tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.3); f) incluye la determinación del mecanismo para evaluar la efectividad de la acción que también se planifica, y puede incluir monitoreo, técnicas de medición (ISO/IEC 27001:2013, 9.1), auditoría interna (ISO/IEC 27001:2013, 9.2) o revisión de la gerencia (ISO/IEC 27001:2013, 9.3).
Documentos de respaldo	ISO 31000:2018, 5.3 to 5.7 ISO/IEC 27003:2017, 6.1.1
A.3.1.2 Evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 8.2
Definiciones relevantes de ISO/IEC 27000	Disponibilidad, confidencialidad, seguridad de la información, integridad, aceptación de riesgos, análisis de riesgos, evaluación de riesgos, criterios de riesgo, identificación de riesgos

Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) planificación del SGSI [ISO/IEC 27001:2013, 6.1.1, 7.5.1 b) y 8.1)]; b) el proceso de evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.2) y los resultados de la evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.2).
Guía práctica de auditoría	Los auditores deberían confirmar que una evaluación de riesgos de seguridad de la información: a) identifica los riesgos de información de seguridad asociados con el SGSI; b) consiste en identificación de riesgos, análisis de riesgos y procesos de evaluación de riesgos.
	Criterios de riesgo [ISO/IEC 27001:2013, 6.1.2 a)]
	Los auditores deberían confirmar que la organización ha establecido y mantiene los criterios de aceptación de riesgos y los criterios para Conducir evaluaciones de riesgos de seguridad de la información. Si bien la organización tiene la libertad de considerar los factores que considere relevantes para establecer sus criterios de riesgo, incluidos los criterios de aceptación de riesgos y los criterios para Conducir evaluaciones de riesgos de seguridad de la información, los auditores deberían evaluar que la organización estableció sus criterios de riesgos, incluidos los criterios de aceptación de riesgos y sus criterios. para Conducir evaluaciones de riesgos de seguridad de la información basadas en decisiones informadas. Es razonable esperar que los criterios de riesgo de la organización se incluyan en la información documentada sobre el proceso de evaluación de riesgos. De lo contrario, la organización debería poder explicar a los auditores qué son. Como mínimo, deberían incluir los criterios de aceptación de riesgos de las organizaciones y los criterios para Conducir evaluaciones de riesgos. NOTA 7: ISO/IEC 27001:2013, 8.2 requiere que las organizaciones realicen evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos. La evaluación de riesgos se puede Conducir en todos los SGSI o en partes de este (este último caso puede mostrar cuándo los cambios significativos tienen un impacto en partes del SGSI y luego se requiere una nueva evaluación de riesgos parcial).

	Consistencia, validez y comparabilidad de los resultados [ISO/IEC 27001:2013, 6.1.2 b)]
	Los auditores deberían confirmar que los resultados de las evaluaciones de riesgos mediante el proceso de evaluación de riesgos de seguridad de la información son consistentes, válidos y comparables. Esta confirmación puede ser realizada por: - preguntando a la organización por qué sus propios resultados de evaluación de riesgos son consistentes, válidos y comparables; - muestreo de la información documentada sobre los resultados de la evaluación de riesgos de seguridad de la información. Para evaluar la consistencia y la reproducibilidad, los auditores pueden verificar si: - riesgos similares en contextos similares han sido evaluados de manera similar; - los riesgos evaluados de manera diferente tienen una justificación para tal diferencia; - los resultados generales de la evaluación son inequívocamente comprensibles. Para evaluar la comparabilidad, los auditores pueden verificar: - cómo se ha evaluado el mismo riesgo en evaluaciones de riesgo anteriores y si es entendible si ha cambiado; - si es inequívocamente comprensible si un riesgo es mayor o menor que otros.
	Identificación de riesgos [ISO/IEC 27001:2013, 6.1.2 c)]
	Los auditores deberían confirmar que la organización ha identificado los riesgos de seguridad de la información asociados con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI. NOTA 8: ISO/IEC 27001:2013 no requiere la identificación de riesgos mediante la identificación de activos, amenazas y vulnerabilidades. Otros métodos de identificación de riesgos son aceptables, como la identificación de riesgos a través de la consideración de eventos y consecuencias.

	Es razonable esperar encontrar una descripción del proceso de identificación de riesgos de la organización en su información documentada sobre el proceso de evaluación de riesgos (ver más abajo). Los factores que la organización puede haber considerado (pero no es necesario) al formular su enfoque para la identificación de riesgos pueden incluir: a) cómo se encuentran, reconocen y describen los riesgos; b) las fuentes de riesgo a considerar. Otros factores que la organización puede haber considerado (pero no necesariamente) son: a) cómo los riesgos pueden crear, mejorar, prevenir, degradar, acelerar o retrasar el logro de los objetivos de seguridad de la información de la organización; los riesgos asociados con no buscar una oportunidad; b) arriesga si su fuente está o no bajo el control de la organización, aunque la fuente o causa del riesgo no sea evidente; c) examen de los efectos indirectos de consecuencias particulares, incluyendo la cascada y los efectos acumulativos; d) considerar una amplia gama de consecuencias, incluso si la fuente o causa del riesgo puede no ser evidente; e) consideración de posibles causas y escenarios que muestran qué consecuencias pueden ocurrir; f) consideración de todas las causas y consecuencias significativas; g) cómo se puede generar una lista completa de riesgos. NOTA 9: El descubrimiento de que se han omitido inadvertidamente grandes cantidades de controles necesarios puede ser indicativo de un proceso de identificación de riesgo débil. Debería confirmarse en el muestreo que toda la información importante dentro del alcance del SGSI se incluye en la evaluación de riesgos. Los auditores deberían verificar que existen riesgos identificados en la información documentada con respecto a los resultados de la

	evaluación de riesgos que están asociados con la pérdida de confidencialidad, integridad y disponibilidad de información dentro del alcance del SGSI. Los objetivos de seguridad de la información de la organización pueden ayudar a los auditores a identificar los riesgos de seguridad de la información. Los auditores también deberían confirmar que: a) para cada riesgo, se han identificado los propietarios del riesgo; b) cada propietario de riesgo tiene la responsabilidad y la autoridad para Gestionar sus riesgos identificados.
	Análisis de riesgos [ISO/IEC 27001:2013, 6.1.2 d)]
	Los auditores deberían confirmar que: a) la organización comprende la naturaleza del riesgo identificado y determina el nivel del riesgo, como análisis de riesgo en el proceso de evaluación de riesgos de seguridad de la información; b) el análisis de riesgos proporciona un insumo para la evaluación de riesgos y las decisiones sobre cómo deberían tratarse los riesgos y sobre el tratamiento, las estrategias y los métodos de riesgo más apropiados. Los auditores también deberían confirmar que la organización ha evaluado las posibles consecuencias y probabilidades asociadas con los riesgos que identificó de conformidad con ISO/IEC 27001:2013, 6.1.2 c) y por lo tanto ha determinado los niveles de riesgo. Es razonable esperar encontrar una descripción del enfoque de la organización para el análisis de riesgos en la información documentada sobre el proceso de evaluación de riesgos y los resultados estarán en la información documentada sobre los resultados de la evaluación de riesgos (ver más abajo). Los auditores deberían consultar las políticas, estrategias y métodos de gestión de riesgos de la organización. El análisis de riesgos puede ser: a) emprendido con diversos grados de detalle, dependiendo del riesgo, el propósito del análisis y la información, datos y recursos disponibles; b) cualitativo, semicuantitativo o cuantitativo o una combinación de estos, dependiendo de las circunstancias.

	Evaluación de riesgos [ISO/IEC 27001:2013, 6.1.2 e)]
	Los auditores deberían confirmar que la organización ha comparado los resultados de su análisis de riesgos con los criterios de aceptación de riesgos de seguridad de la información para determinar la aceptabilidad de los riesgos identificados. Los auditores también deberían confirmar que los resultados de la (s) evaluación (es) de riesgo revelan como evidencia que los criterios de aceptación de riesgos se han aplicado correctamente y que los riesgos identificados y analizados han sido priorizados para el tratamiento. En más detalles, los auditores deberían revisar que la evaluación de riesgos: a) ayuda a tomar decisiones, basadas en los resultados del análisis de riesgos, sobre cómo los riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento; b) implica comparar el nivel de riesgo encontrado durante el proceso de análisis con los criterios de riesgo de seguridad de la información establecidos cuando se consideró el contexto. Los auditores también deberían evaluar que las decisiones: a) tener en cuenta el contexto más amplio del riesgo; b) tener en cuenta los requisitos de interesados pertinentes partes, incluyendo legales, regulatoria y otros requisitos.
	Información documentada [ISO/IEC 27001:2013, 6.1.2 y 8.2]
	Los auditores deberían confirmar que existe información documentada sobre el proceso de evaluación de riesgos. Sería razonable esperar que la información documentada sobre el proceso de evaluación de riesgos de seguridad de la información contenga: a) una definición de los criterios de riesgo, incluidos los criterios de aceptación del riesgo y los criterios para Conducir evaluaciones de riesgos de seguridad de la información; b) justificación de la coherencia, validez y comparabilidad de los resultados; c) una descripción del proceso de identificación del riesgo (incluida la identificación de los propietarios del riesgo);

	d) una descripción del proceso para analizar los riesgos de seguridad de la información (incluida la evaluación de las posibles consecuencias, la probabilidad realista y el nivel de riesgo resultante); e) una descripción del proceso para comparar los resultados con los criterios de riesgo y la priorización de riesgos para el tratamiento del riesgo. NOTA 10: Cada uno de los elementos mencionados corresponde a un requisito ISO/IEC 27001, por lo que es razonable que se encuentre información sobre ellos en la información documentada sobre el proceso de evaluación de riesgos.
Documentos de respaldo	ISO 31000:2018, 5.3, 5.4, 5.7 ISO/IEC 27003:2017, 6.1.2, 8.2
A.3.1.3 Tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 8.3, Anexo A
Definiciones relevantes de ISO/IEC 27000	Control, objetivo de control, información documentada, seguridad de la información, riesgo residual, evaluación de riesgos, criterios de riesgo, propietario del riesgo, tratamiento del riesgo
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) planificación para el SGSI; b) el proceso de tratamiento de riesgos de seguridad de la información; c) los resultados del tratamiento del riesgo de seguridad de la información; d) la Declaración de Aplicabilidad.
Guía práctica de auditoría	**Tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.3)**
	Los auditores deberían confirmar que la organización modifica los riesgos de seguridad de la información como un proceso de tratamiento de riesgos de seguridad de la información. Los auditores también deberían revisar que el tratamiento del riesgo de seguridad de la información implica:

	a) seleccionar una o más opciones para modificar los riesgos de seguridad de la información e implementar esas opciones, que proporcionan o modifican los controles; b) un proceso cíclico de evaluación de la efectividad de ese tratamiento
	Seleccione las opciones adecuadas de tratamiento de riesgos de seguridad de la información [ISO/IEC 27001:2013, 6.1.3 a)]
	Los auditores deberían confirmar que la información documentada sobre el proceso de tratamiento de riesgos contiene una descripción del método que utiliza la organización para seleccionar las opciones adecuadas de tratamiento de riesgos de seguridad de la información. Los auditores también deberían confirmar que esta descripción corresponde a lo que la organización realmente realiza. Tenga en cuenta que ISO/IEC 27000:2018, 3.72, Nota 1 enumera siete opciones de tratamiento de riesgo y hay una nota que hace referencia a ISO 31000 en ISO/IEC 27001:2013, 6.1.3 de donde se derivan. Los auditores deberían verificar la consistencia entre los criterios de riesgo y el plan de tratamiento de riesgos. La organización debería poder explicar las decisiones que ha tomado con respecto a las opciones de tratamiento de riesgo, incluso si no están documentadas. Los auditores deberían revisar las opciones de tratamiento de riesgos seleccionadas por la organización. Los auditores también deberían revisar la idoneidad de las opciones de tratamiento de riesgo seleccionadas. Los auditores deberían verificar si los cambios recientes (por ejemplo, nuevos sistemas de TI o procesos comerciales) se han incorporado adecuadamente en la evaluación de riesgos y las decisiones de tratamiento de riesgos.
	Determine todos los controles necesarios [ISO/IEC 27001:2013, 6.1.3 b)]
	Los auditores deberían confirmar que la información documentada sobre el proceso de tratamiento de riesgos contiene una descripción del método que utiliza la organización para determinar los controles de seguridad de la información necesarios. Los auditores también deberían confirmar que esta descripción corresponde a lo que realmente hace la organización.

	Es un requisito [ISO/IEC 27001:2013, 6.1.3 d)] que la Declaración de Aplicabilidad contenga los controles necesarios. Los controles necesarios no necesitan ser ISO/IEC 27001:2013, controles del Anexo A. Pueden ser controles específicos del sector (como se define en los estándares específicos del sector, como ISO/IEC 27011, ISO/IEC 27017). También pueden ser "controles personalizados", ya que las organizaciones pueden diseñar sus propios o identificados de cualquier fuente [véase ISO/IEC 27001:2013, 6.1.3 b)]. Todos los controles determinados para implementar las opciones de tratamiento de riesgos deberían incluirse en la Declaración de Aplicabilidad. Además, cualquier control personalizado debería definirse explícitamente como requisito e implementación.
	Comparar con el anexo A [ISO/IEC 27001 :2013, 6.1.3 c)]
	El cumplimiento de este requisito se evidencia a través de la revisión de la Declaración de Aplicabilidad como se describe a continuación.
	Producir una Declaración de Aplicabilidad [ISO/IEC 27001:2013, 6.1.3 d)]
	Los auditores deberían verificar que la Declaración de Aplicabilidad contenga: a) los controles necesarios según lo determinado por el proceso de aplicación de ISO/IEC 27001:2013, 6.1.3 b) y c); b) la justificación para su inclusión (por ejemplo, por referencia a las opciones de tratamiento de riesgo donde se usa); c) si se implementan o no los controles necesarios; d) una justificación para todos los controles excluidos del Anexo A (por ejemplo: 1) el control se aplica en el contexto de una actividad que la organización no realiza; 2) la organización utiliza un control personalizado que elimina la necesidad de un control del Anexo A; 3) la organización utiliza un control personalizado que sirve para el mismo propósito que el control del Anexo (consulte ISO/IEC 27003 para obtener más información);

	e) controles específicos del sector relevantes, que se designarán como controles necesarios o se tratarán de la misma manera que los controles excluidos del Anexo A. Por lo tanto, los auditores deberían confirmar la consistencia entre los controles necesarios para Conducir las opciones de tratamiento de riesgo seleccionadas y la Declaración de Aplicabilidad.
	Formular un plan de tratamiento de riesgos [ISO/IEC 27001:2013, 6.1.3 e)]
	Los auditores deberían confirmar que la información documentada sobre el proceso de tratamiento de riesgos contiene una descripción del método que utiliza la organización para producir su plan de tratamiento de riesgos. Los auditores también deberían confirmar que el plan de tratamiento de riesgos se formula a partir de los resultados de ISO/IEC 27001:2013, 6.1.3 a) a c). Los auditores deberían confirmar además que la información provista en el plan de tratamiento incluye enlaces a: a) los riesgos que aborda el plan; b) controles necesarios; c) cómo se espera que los controles necesarios modifiquen el riesgo para que se cumplan los criterios de aceptación del riesgo; d) los propietarios del riesgo; NOTA 11: Los propietarios del riesgo son responsables de aprobar el plan de tratamiento del riesgo y aceptar el riesgo residual. e) opciones de tratamiento de riesgo seleccionadas; f) el estado de implementación de los controles necesarios; g) las razones para la selección de opciones de tratamiento, incluidos los beneficios esperados que se obtendrán; h) acciones propuestas, incluidas las personas responsables, los plazos y el calendario; i) requisitos de recursos, incluidas contingencias;

	j) medidas de desempeño y limitaciones; k) informes y seguimiento. Los auditores deberían revisar que el plan de tratamiento de riesgos tenga en cuenta el establecimiento de objetivos y los procesos de gestión de la organización y se discuta con las partes interesadas relevantes.
	Obtener la aprobación del propietario del riesgo [ISO/IEC 27001:2013, 6.1.3 f)]
	Los auditores deberían confirmar que la organización: a) identifica a los propietarios de riesgos apropiados; b) documenta los riesgos residuales; c) obtiene la aprobación de los propietarios de riesgos para el plan de tratamiento de riesgos de seguridad de la información y la aceptación de los riesgos residuales.
	Información documentada
	Los auditores deberían confirmar que existe información documentada sobre el proceso de tratamiento de riesgos. Sería razonable esperar que la información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información contenga descripciones de: a) el método para seleccionar opciones apropiadas de tratamiento de riesgos de seguridad de la información; b) el método para determinar los controles necesarios; c) cómo se utiliza ISO/IEC 27001:2013, Anexo A para determinar que los controles necesarios no se han pasado por alto inadvertidamente; d) cómo el SOA es producido; e) cómo el plan de tratamiento del riesgo es producido; f) cómo se obtiene la aprobación de los propietarios del riesgo.

	NOTA 12: No existe un requisito particular para el contenido o el formato del plan de tratamientos de riesgo de una organización.
Documentos de respaldo	ISO 31000:2018, 5.5, 5.7 ISO/IEC 27003:2017, 6.1.3, 8.3 ISO/IEC 27006
A.3.2 Objetivos de seguridad de la información y planificación para alcanzarlos (ISO/IEC 27001:2013, 6.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.1, 5.2, 7.1, 7.3, 7.4, 7.5, 9.1, 9.3, 10.2
Definiciones relevantes de ISO/IEC 27000	Seguridad de la información, objetivo
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre objetivos de seguridad de la información y planes para lograrlos.
Guía práctica de auditoría	Se observa que existen vínculos entre los objetivos de seguridad de la auditoría información y la planificación para alcanzarlos (ISO/IEC 27001:2013, 6.2) con el liderazgo y el compromiso IEC 27001:2013, 5.1) y la política IEC 27001:2013, 5.2). Los auditores deberían confirmar que: a) los objetivos de seguridad de la información se establecen en las funciones y niveles relevantes de la organización; b) los objetivos de seguridad de la información se especifican de una manera que permita determinar su cumplimiento; c) los objetivos son medibles, si corresponde (puede haber situaciones en las que no sea factible medir un objetivo de seguridad de la información); d) el estado y el progreso de los objetivos de seguridad de la información y los planes para alcanzarlos se verifican periódicamente de acuerdo con los requisitos de monitoreo, medición, análisis y evaluación (ISO/IEC 27001:2013, 9.1) y se actualizan según corresponda, de acuerdo con los requisitos de mejora continua (ISO/IEC 27001:2013, 10.2); e) los objetivos de seguridad de la información y los planes para alcanzarlos se comunican de acuerdo con los requisitos de la comunicación (ISO/IEC 27001:2013, 7.4);

	f) la información documentada de los objetivos se crea y controla de acuerdo con los requisitos de la información documentada (ISO/IEC 27001:2013, 7.5). Los auditores también deberían verificar que: a) se determinan las acciones requeridas para lograr los objetivos de seguridad de la información (es decir, "qué") y el plazo asociado (es decir, "cuándo"); b) la asignación de responsabilidad para hacerlo (es decir, "quién") se establece de acuerdo con los requisitos de los roles, responsabilidades y autoridades de la organización (ISO/IEC 27001:2013, 5.3); c) los requisitos de seguridad de la información aplicables y los resultados de la evaluación de riesgos y el tratamiento de riesgos se tienen en cuenta en los objetivos y la planificación para alcanzarlos; d) cualquier necesidad de presupuestos, habilidades especializadas, tecnología o infraestructura, por ejemplo, para lograr los objetivos se determina y proporciona de acuerdo con los requisitos de recursos (ISO/IEC 27001:2013, 7.1); e) un mecanismo para evaluar los resultados generales de lo que se logró se determina de acuerdo con los requisitos de monitoreo, medición, análisis y evaluación (ISO/IEC 27001:2013, 9.1) y se informa de acuerdo con la revisión de la gerencia (ISO/IEC 27001:2013, 9.3).
Documentos de respaldo	ISO/IEC 27003:2017, 6.2
A.4 Soporte (ISO/IEC 27001:2013, clausula 7)	
A.4.1 Recursos (ISO/IEC 27001:2013, 7.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.1, 6.2, 7.2
Definiciones relevantes de ISO/IEC 27000	Mejora continua, sistema de gestión
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre los recursos que la organización necesita para:

	a) establecer e implementar el SGSI (incluidas sus operaciones y controles); b) mantener y mejorar continuamente el SGSI. Los recursos pueden incluir: a) una persona; b) habilidades o conocimientos especializados; c) infraestructura organizacional (por ejemplo, edificios, líneas de comunicación, entre otros); d) tecnología; e) información, otros activos asociados con la información y las instalaciones de procesamiento de información; f) dinero (por ejemplo, efectivo, valores líquidos y líneas de crédito).
Guía práctica de auditoría	Los auditores deberían confirmar que la organización anticipa, determina y asigna los recursos necesarios para establecer e implementar el SGSI (incluidas sus operaciones y controles), así como los necesarios para su mantenimiento y mejora continua.
Documentos de respaldo	ISO 31000:2018, 4.3.5
A.4.2 Competencia (ISO/IEC 27001:2011, 7.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.3, 7.1, 7.5.1 Note, 9.1 d) y e), 9.2 e)
Definiciones relevantes de ISO/IEC 27000	Competencia, efectividad
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información relevante: a) roles organizacionales, responsabilidades y autoridades; b) descripciones de trabajo; c) competencia requerida;

	d) registros de educación; e) programas de capacitación, cursos y actividades educativas; f) registros de acciones tomadas para adquirir y retener la competencia g) necesaria; h) evaluación de su efectividad. ISO/IEC 27001:2013, 7.2 amplía el alcance de la competencia a las personas que no son miembros de la organización. El requisito especifica que están "trabajando bajo el control de la organización". Los ejemplos pueden incluir subcontratistas y trabajadores voluntarios. La evidencia de auditoría solicitada a un tercero debería restringirse a la evidencia de las funciones y actividades realizadas para la organización del SGSI
Guía práctica de auditoría	Los auditores deberían confirmar que la organización: a) determina: 1) las personas que realizan trabajos bajo su control que afectan su desempeño de seguridad de la información; 2) el conocimiento y las habilidades de las personas para lograr los resultados previstos; 3) la capacidad de las personas para aplicar los conocimientos y habilidades para lograr los resultados previstos; b) asegura que estas personas tengan la capacidad sobre la base de una educación, capacitación o experiencia apropiadas; c) cuando corresponda, toma medidas para adquirir la capacidad necesaria y evaluar la efectividad de las acciones tomadas.
Documentos de respaldo	ISO/IEC 27003:2017, 7.2 ISO/IEC 27021:2017, Annex A
A.4.3 Conciencia (ISO/IEC 27001:2013, 7.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.1 d), 5.2, 9.1, 9.2, 10.1, 10.2

Definiciones relevantes de ISO/IEC 27000	Conformidad, efectividad, desempeño, política
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) política de seguridad de la información; b) objetivos de seguridad de la información; c) desempeño de seguridad de la información; d) no conformidad y acción correctiva; e) roles organizacionales, responsabilidades y autoridades; f) descripciones de trabajo; g) programas de sensibilización y material de capacitación, cuando corresponda.
Guía práctica de auditoría	Los auditores deberían confirmar que las personas que trabajan bajo el control de la organización conocen: a) la política de seguridad de la información; b) su contribución a la efectividad del SGSI, incluidos los beneficios del rendimiento mejorado de la seguridad de la información; c) las implicaciones de no cumplir con los requisitos del SGSI. Los auditores deberían entrevistar a un número apropiado de personas como muestra para confirmar que conocen esta información. El conocimiento de la política no debería entenderse como que necesita ser memorizada; más bien, las personas deberían conocer los compromisos políticos clave y su papel para cumplirlos. Los auditores pueden encontrar evidencia de conciencia de seguridad de la información también en iniciativas de concienciación y capacitación no dedicadas a la seguridad de la información. Estas actividades pueden estar estrechamente relacionadas con las actividades de comunicación de la alta dirección [ISO 27001:2013, 5.1 d) y 7.4].

Documentos de respaldo	ISO/IEC 27003:2017, 7.3
A.4.4 Comunicación (ISO/IEC 27001:2013, 7.4)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.1, 5.2, 5.3, 6.2, 9.2
Definiciones relevantes de ISO/IEC 27000	Política
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre a) política de seguridad de la información; b) roles organizacionales, responsabilidades y autoridades; c) el proceso de evaluación de riesgos de seguridad de la información; d) el proceso de tratamiento de riesgos de seguridad de la información; e) objetivos de seguridad de la información; f) información de que los procesos se han llevado a cabo según lo previsto; g) los resultados de las evaluaciones de riesgos de seguridad de la información; h) los resultados del tratamiento del riesgo de seguridad de la información; i) desempeño del SGSI; j) resultados de auditorías k) resultados de las revisiones de la gerencia.
Guía práctica de auditoría	Los auditores deberían confirmar que las necesidades de comunicación de la organización se identifican, implementan y mantienen de manera efectiva a lo largo de los requisitos de comunicación de ISO/IEC 27001.

	Ejemplos de evidencia pueden incluir: a) respuestas documentadas en el acta de una reunión, o b) un plan de comunicaciones formal, procedimientos y resultados documentados, o c) entrevistas con personas asignadas a roles definidos para demostrar que saben, para la comunicación relevante a sus roles, sobre qué, cuándo, a quién comunicarse, quién tiene las autoridades para dicha comunicación y cómo es el proceso por el cual La comunicación se ve afectada. Dicha evidencia se puede complementar con: a) información de comunicación sobre lo siguiente: 1) 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; 2) política; 3) responsabilidades y autoridades; 4) desempeño del SGSI; 5) objetivos; 6) contribución a la efectividad del SGSI, incluidos los beneficios de un mejor desempeño; 7) implicaciones de no cumplir con los requisitos del SGSI; 8) resultados de auditorías; b) un plan de comunicación formal, procedimientos documentados y resultados. Los auditores deberían verificar que la organización haya determinado sus necesidades de comunicación relacionadas con el SGSI. Por ejemplo, estos pueden incluir transparencia, adecuación, credibilidad, capacidad de respuesta, claridad y protección.

	La comunicación puede ser verbal o escrita, unidireccional o bidireccional, interna o externa.
Documentos de respaldo	ISO 31000:2018, 4.3.6, 4.3.7 ISO/IEC 27003:2017, 7.4
A.4.5 Información documentada (ISO/IEC 27001:2013, 7.5)	
A.4.5.1 General (ISO/IEC 27001:2013, 7.5.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1
Definiciones relevantes de ISO/IEC 27000	Información documentada
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información creada, controlada y/o mantenida en un SGSI, que incluye: a) alcance del sistema de gestión; b) política; c) objetivos; d) evidencia de competencia; e) información de origen externo necesaria para la planificación y operación del sistema de gestión; f) proceso de evaluación de riesgos de seguridad de la información; g) proceso de tratamiento de riesgos de seguridad de la información; h) Declaración de Aplicabilidad; i) información necesaria para tener confianza en que los procesos y los controles determinados se han llevado a cabo según lo planeado; j) resultados de la evaluación de riesgos de seguridad de la información; k) resultados del tratamiento del riesgo de seguridad de la información;

	l) resultados de monitoreo, medición, análisis y evaluación; m) programa de auditoría interna y evidencia de su implementación; n) resultados de auditoría interna; o) resultados de la revisión de la gerencia; p) naturaleza de las no conformidades y acciones tomadas; q) resultados de acciones correctivas. Se puede utilizar la información documentada, creada originalmente para fines distintos al cumplimiento de los requisitos de ISO/IEC 27001.
Guía práctica de auditoría	Los auditores deberían confirmar que el SGSI de la organización incluye: a) información documentada requerida por ISO/IEC 27001; b) información documentada determinada por la organización como necesaria para la efectividad del SGSI. La frase "información documentada como evidencia de ..." implica el antiguo término "registro". Los auditores deberían confirmar que la organización determina qué información documentada necesita más allá de lo que se requiere explícitamente por ISO/IEC 27001 para la efectividad de su SGSI. Los factores que debería tener en cuenta se enumeran en la fila de evidencia de auditoría. El término "información documentada" se refiere a la información que ISO/IEC 27001 determina que es necesaria para controlar y mantener en cualquier formato o medio (véase ISO/IEC 27001:2013, 7.5.3). El auditor debería confirmar que la información documentada se crea y controla de acuerdo con los requisitos de ISO/ IEC 27001:2013, 7.5.2 y 7.5.3.
Documentos de respaldo	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.1

A.4.5.2 Creación y actualización (ISO/IEC 27001:2013, 7.5.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1
Definiciones relevantes de ISO/IEC 27000	Información documentada
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) atributos comunes que permiten una identificación clara y única; b) formato y medios utilizados; c) fecha de la última revisión o actualización; d) historial de cambios; e) identidad del revisor y aprobador.
Guía práctica de auditoría	Los auditores deberían confirmar que, al crear y actualizar información documentada, la organización garantiza: a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia); b) formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico); c) revisión y aprobación de la idoneidad y adecuación de la información documentada. NOTA 13: La identificación, el formato y los medios utilizados para la información documentada son la elección de la organización que implementa ISO/IEC 27001; no es necesario que tenga la forma de un formato de texto o un manual en papel. Los auditores deberían aprovechar la oportunidad de llevar a cabo estas tareas de auditoría siempre que se presente a la auditoría información documentada dentro del alcance del SGSI. No necesitan Conducirse cada vez solo un número suficiente para confirmar la conformidad con ISO/IEC 27001:2013, 7.5.2.
Documentos de respaldo	ISO/IEC 27003:2017, 7.5.2
A.4.5.3 Control de información documentada (ISO/IEC 27001:2013, 7.5.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.3, 5.2 e), 6.1.2, 6.1.3, 6.2, 7.2 d), 8.1, 8.2, 8.3, 9.1, 9.2 g), 9.3, and 10.1

Definiciones relevantes de ISO/IEC 27000	Información documentada
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre las siguientes actividades: a) distribución, acceso, recuperación y uso; b) almacenamiento y preservación, incluida la preservación de la legibilidad; c) control de cambios (por ejemplo, control de versiones); d) retención y disposición; e) estructura y configuración de la biblioteca de información documentada.
Guía práctica de auditoría	Los auditores deberían confirmar que la información documentada requerida por el SGSI y por ISO/IEC 27001 se controla para garantizar que: a) está disponible y es adecuado para su uso, donde y cuando sea necesario; b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad). El auditor debería confirmar que la organización aborda las siguientes actividades, según corresponda: a) distribución, acceso, recuperación y uso; b) almacenamiento y preservación, incluida la preservación de la legibilidad (en formatos digitales u otros o escritos a mano); c) control de cambios (por ejemplo, control de versiones); d) retención y disposición. Los auditores deberían aprovechar la oportunidad de llevar a cabo estas tareas de auditoría siempre que se presente a la auditoría información documentada dentro del alcance del SGSI. No tienen que Conducirse cada vez, solo un número suficiente para confirmar la conformidad con ISO/IEC 27001:2013, 7.5.3.

Documentos de respaldo	ISO 31000:2018, 5.7 ISO/IEC 27003:2017, 7.5.3
A.5 Operación (ISO/IEC 27001:2013, clausula 8)	
A.5.1 Planificación y control operacional (ISO/IEC 27001:2013, 8.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.4, 6.1.1, 6.1.2, 6.1.3, 6.2, 7.5.1, 9.1, and 9.2
Definiciones relevantes de ISO/IEC 27000	Consecuencia, seguridad de la información, objetivo, organización, tercerización, proceso, requerimiento
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información que sea: a) necesario para que la organización tenga confianza en que los procesos de control operativo se han llevado a cabo según lo planificado se crea y controla (ISO/IEC 27001:2013, 8.1); b) determinado por la organización como necesario para la efectividad del SGSI [ISO/IEC 27001:2013, 7.5.1 b)]; c) sobre la planificación del SGSI (ISO/IEC 27001:2013, 6.1.1); d) sobre objetivos de seguridad de la información (ISO/IEC 27001:2013, 6.2).
Guía práctica de auditoría	Los auditores deberían confirmar que la organización planifica, implementa y controla los procesos necesarios para cumplir con los requisitos de seguridad de la información dentro de las operaciones de la organización para asegurarse de que se cumplan los requisitos de ISO/IEC 27001 y se aborden los riesgos y oportunidades prioritarios. Los auditores deberían confirmar que el control operativo incluye los métodos y los controles de seguridad de la información implementados para garantizar que las operaciones, actividades o equipos comerciales cumplan con las condiciones especificadas, los estándares de desempeño o los límites de cumplimiento normativo y, de ese modo, logren efectivamente el resultado previsto del SGSI. Estos controles establecenlos requisitos técnicos necesarios para lograr la funcionalidad óptima deseada para los procesos comerciales, como las especificaciones técnicas o los parámetros operativos o una metodología prescrita. La revisión debería Conducirse para las situaciones para las que se requiere el control operativo y los controles de seguridad de la

	información, relacionados con los procesos comerciales donde la ausencia del control operativo y los controles de seguridad de la información podrían conducir a desviaciones de la política y los objetivos o presentar un riesgo inaceptable. Estas situaciones pueden estar relacionadas con operaciones comerciales, actividades o procesos, producción, instalación o servicio, mantenimiento o contratistas, proveedores o vendedores. El grado de control ejercido variará dependiendo de muchos factores, incluidas las funciones realizadas, su importancia o complejidad, las posibles consecuencias de la desviación o variabilidad o la competencia técnica involucrada frente a lo que está disponible. Los auditores deberían verificar que la organización: a) implementa las acciones determinadas en "acciones para abordar riesgos y oportunidades" (ISO/IEC 27001:2013, 6.1); b) implementa los planes para alcanzar los objetivos de seguridad de la información determinados en los objetivos de seguridad de la información y la planificación para alcanzarlos (ISO/IEC 27001:2013, 6.2); c) crea y controla la documentación necesaria para tener la confianza de que los procesos de control operativo y los controles de seguridad de la información se han llevado a cabo según lo planeado de acuerdo con los requisitos de información documentada (ISO/IEC 27001:2013, 7.5); d) controla los cambios planificados y revisa las consecuencias de los cambios no deseados, para prevenir o minimizar lo contrario la oportunidad técnicas requisitos son no cumplen o nuevos riesgos se introdujeron; e) toma las acciones necesarias para abordar los efectos indeseables resultantes cuando fallan los controles operativos; f) asegura que los procesos tercerizados se determinan y controlan, es decir, aplica el control de las operaciones bajo consideraciones tales que el grado de control puede limitarse a un control o influencia parcial y no pretende cambiar ninguna relación legal con el externo entidad que realiza el proceso tercerizado.
Documentos de respaldo	ISO/IEC 27003:2017, 8.1

A.5.2 Evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 6.1.2
Definiciones relevantes de ISO/IEC 27000	Seguridad de información
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) planificación para el SGSI (ISO/IEC 27001:2013, 6.1.1); b) el proceso de evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 6.1.2); c) los resultados de la evaluación de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.2); d) la Declaración de Aplicabilidad; e) los planes de tratamiento de riesgos.
Guía práctica de auditoría	Los auditores deberían confirmar que el proceso de evaluación de riesgos de seguridad de la información definido y aplicado en (ISO/IEC 27001:2013, 6.1) se implementa e integra en las operaciones de la organización y se realiza a intervalos planificados o cuando se proponen u ocurren cambios significativos, tomando cuenta de los criterios establecidos en ISO/IEC 27001:2013, 6.1.2 a). Los auditores deberían evaluar que: a) los intervalos planificados a los que se realiza la evaluación de riesgos son apropiados para el SGSI; b) cuando se producen cambios significativos en el SGSI (o su contexto) o incidentes de seguridad de la información, la organización determina cuáles de estos cambios o incidentes requieren una evaluación adicional del riesgo de seguridad de la información y cómo se activan estas evaluaciones. Para obtener información adicional, consulte la guía práctica de auditoría de A.3.1.2.
Documentos de respaldo	ISO 31000:2018, 5.4.1 ISO/IEC 27003:2017, 8.2

	ISO/IEC 27005
A.5.3 Tratamiento de riesgos de seguridad de la información (ISO/IEC 27001:2013, 8.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 6.1.3, Anexo A
Definiciones relevantes de ISO/IEC 27000	Control, objetivo de control, información documentada, seguridad de la información, riesgo residual, evaluación de riesgos, criterios de riesgo, propietario del riesgo, tratamiento del riesgo
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) planificación para el SGSI; b) el proceso de tratamiento de riesgos de seguridad de la información; c) los planes de tratamiento de riesgos; d) los resultados del tratamiento del riesgo de seguridad de la información; e) la Declaración de Aplicabilidad.
Guía práctica de auditoría	Los auditores deberían confirmar que el proceso de tratamiento de riesgos de seguridad de la información definido y aplicado en "Planificación del SGSI" (ISO/IEC 27001:2013, 6.1) se implementa e integra en las operaciones de la organización, y se realiza después de cada iteración de la seguridad de la información proceso de evaluación de riesgos (ISO/IEC 27001:2013, 8.2) o cuando la implementación de (partes de) el tratamiento de riesgos ha fallado. Para obtener información adicional, consulte la guía práctica de auditoría de A.3.1.3.
Documentos de respaldo	ISO 31000:2018, 5.5 ISO/IEC 27003:2017, 8.3 ISO/IEC 27005
A.6 Evaluación de desempeño (ISO/IEC 27001:2013, clausula 9)	
A.6.1 Monitoreo, medición, análisis y evaluación (ISO/IEC 27001:2013, 9.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.3 b), 6.1.1 e), 6.2
Definiciones relevantes de ISO/IEC 27000	Mejora continua, efectividad, medición, monitoreo, desempeño, evento de seguridad de información, incidente de seguridad de información, necesidad de información, medida

Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre los resultados del monitoreo, medición, análisis y evaluación (véase ISO/IEC 27001:2013, 9.1). La evidencia también se puede obtener a través de información documentada u otra información sobre: a) objetivos de seguridad de la información en funciones y niveles relevantes; b) planificar cómo lograr los objetivos de seguridad de la información; c) el estado y la medida en que se cumplen los objetivos de seguridad de la información; d) informar sobre el desempeño del SGSI a la alta gerencia [véase ISO/IEC 27001:2013, 5.3 b)]; e) resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos; f) los métodos de seguimiento, medición, análisis y evaluación; g) programa (s) de auditoría interna y los resultados de la auditoría; h) revisiones de la gestionación y los resultados de las revisiones de la gestionación; i) informes de eventos de seguridad de la información (véase ISO/IEC 27001:2013, A.16.1.2); j) informes de debilidades de seguridad de la información (véase ISO/IEC 27001:2013, A.16.1.3); k) informes de incidentes de seguridad de la información (véase ISO/IEC 27001:2013, A.16.1.4).
Guía práctica de auditoría	Los auditores deberían confirmar que la organización tiene: a) evaluó el desempeño de seguridad de la información y la efectividad de su SGSI; b) ha determinado así:

	1) qué se debería monitorear y medir (cualitativa y cuantitativamente), incluidos los procesos y controles de seguridad de la información; 2) los métodos de monitoreo, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos; 3) cuándo se Conducirá el monitoreo y la medición; 4) quién realiza el monitoreo y la medición; 5) cuándo se analizarán y evaluarán los resultados del monitoreo y la medición; 6) quién realiza el análisis y la evaluación de estos resultados. Los auditores deberían revisar el desempeño de la seguridad de la información utilizando información documentada como evidencia, como planes, informes sobre el desempeño del SGSI a la alta gerencia, los resultados de la revisión de la gerencia, informes de auditoría interna y eventos de seguridad de la información, informes de incidentes de debilidad. Los auditores deberían evaluar en qué medida las no conformidades, los errores de procesamiento, las infracciones de seguridad de la información y otros incidentes se predicen, detectan, informan y abordan. Los auditores deberían determinar si la organización evalúa la eficacia de las acciones y cómo las realiza para abordar los riesgos y las oportunidades para garantizar que los controles de seguridad de la información identificados en el tratamiento del riesgo se implementen de manera efectiva y estén en funcionamiento. Los auditores también deberían evaluar la evaluación del rendimiento de la seguridad de la información para ser utilizada para impulsar mejoras continuas del SGSI. Los auditores también deberían confirmar que los cambios a considerar (ISO/IEC 27001:2013, 8.1 y 8.2) a partir de los resultados se reflejan en los procesos de evaluación de riesgos y procesos de tratamiento de riesgos. Además, los auditores deberían confirmar que se ha actualizado la información documentada relacionada con las acciones para abordar el riesgo y las oportunidades. Los auditores deberían revisar que la información de las características que se monitorean o miden, analizan y evalúan es necesaria y suficiente para juzgar en qué medida se realizan las actividades

	planificadas del SGSI y se logran sus resultados planificados. Los auditores deberían confirmar que la información obtenida a través del monitoreo o medición, análisis y evaluación se presenta a la alta dirección de acuerdo con los requisitos de la revisión por la dirección (ISO/IEC 27001:2013, 9.3). NOTA 14: Si una organización sigue la guía dada en ISO/IEC 27004, además de "necesidad de información", puede usar los términos "medida de desempeño" y "medida de efectividad".
Documentos de respaldo	ISO/IEC 27004
A.6.2 Auditoría interna (ISO/IEC 27001:2013, 9.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 9.3
Definiciones relevantes de ISO/IEC 27000	Auditoría, alcance de la auditoría, competencia.
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) un programa o programas de auditoría interna; b) planes de auditoría interna; c) resultados de la auditoría interna; d) competencia de los auditores internos; e) resultados de las revisiones de gestión.
Guía práctica de auditoría	NOTA 15: Este subcapítulo proporciona orientación para la auditoría externa o la autocomprobación o la evaluación de evaluación de pares con respecto a la auditoría interna. Los auditores deberían confirmar que la organización planifica, implementa y mantiene un programa de auditoría interna con el fin de proporcionar información sobre si el SGSI cumple con los requisitos de ISO/IEC 27001 y cualquier requisito adicional relacionado con el SGSI que la organización se impone y que el SGSI está siendo eficaz implementado y mantenido según lo planeado. Los auditores deberían verificar que el programa de auditoría interna sea tal que:

	a) las auditorías internas se planifican y programan en función de la importancia de los procesos auditados y los resultados de auditorías anteriores; b) se establece el enfoque para planificar y Conducir auditorías internas; c) las funciones y responsabilidades dentro del programa de auditoría se asignan teniendo en cuenta la integridad e independencia del proceso de auditoría interna; d) los objetivos de auditoría, los criterios de auditoría y el alcance de auditoría se establecen para cada auditoría planificada; e) está diseñado para proporcionar información para confirmar que el SGSI cumple con: 1) los requisitos de ISO/IEC 27001; 2) los requisitos propios de la organización; f) está diseñado para proporcionar información para confirmar que el SGSI se implementa y mantiene de manera efectiva. Un ejemplo de un criterio de auditoría es una referencia (por ejemplo, políticas, procedimientos y requisitos) contra la cual se compararán registros relevantes y verificables, declaraciones de hechos u otra información. Los ámbitos de auditoría pueden incluir descripciones de las ubicaciones físicas, unidades organizativas, actividades y procesos, así como el período de tiempo cubierto para las auditorías en cuestión. Los auditores deberían confirmar que el programa de auditoría interna y las auditorías sean planificadas e implementadas y mantenidas por personal interno, o que sean gestionadas por personas externas que actúen en nombre de la organización. En cualquier caso, los auditores deberían confirmar que la selección de las personas responsables de la gestión de la interna de auditoría programa y los auditores que llevan a cabo el interior auditorías se reúnen competencia (véase la norma ISO/IEC 27001:2013, 7.2 y 9.2) Requisitos y directrices (véase ISO/IEC 27007:2013,7.2) Los auditores deberían confirmar que los resultados de las auditorías internas se informan a la dirección responsable de las funciones / unidad auditada y a cualquier otra persona que se considere apropiada

	de acuerdo con los requisitos de comunicación (ISO/IEC 27001:2013, 7.4). Los auditores deberían confirmar que la información, incluidos los resultados, sobre los resultados de la auditoría interna se revisa de acuerdo con los requisitos de la revisión de la gestión (véase ISO/IEC 27001:2013, 9.3).
Documentos de respaldo	Esta Norma Técnica Peruana, es decir, NTP-ISO/IEC 27007 ISO/IEC TS 27008 ISO/IEC 17021-1:2015, 9.3.1.2.2 g), 9.3.1.3 e), 9.4.8.3 a), 9.6.2.2 a) ISO/IEC 27006:2015, 9.1.5.1, 9.3.1.2.2 h), 9.5.1, 9.6.2.1.1 a)
A.6.3 Revisión por la dirección (ISO/IEC 27001:2013, 9.3)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 4.1, 4.2, 8.1.2, 8.1.3, 9.1, 9.2, 10.1, and 10.2
Definiciones relevantes de ISO/IEC 27000	Mejora continua, efectividad, desempeño
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) conducir las revisiones a intervalos planificados; b) el estado de las acciones de revisiones gestionativas anteriores; c) cambios en los problemas externos e internos que son relevantes para el SGSI; d) retroalimentación sobre el desempeño la seguridad de la información, incluyendo tendencias en no conformidades y acciones correctivas, resultados de monitoreo y medición, resultados de auditoría y cumplimiento de objetivos de seguridad de la información; e) comentarios de las partes interesadas; f) resultados de la evaluación de riesgos y el estado del plan de tratamiento de riesgos; g) oportunidades de mejora continua.
Guía práctica de auditoría	Los auditores deberían confirmar que la alta dirección ha llevado a cabo revisiones de la gerencia de acuerdo con un cronograma planificado de revisiones, revisando la información a cubrir y proporcionando los resultados esperados.

	Los auditores deberían evaluar a través de la auditoría que la alta dirección se involucre personalmente en esta revisión, llevando a cabo este mecanismo para impulsar cambios en el SGSI y prioridades de mejora continua directa, particularmente en relación con los problemas cambiantes en el contexto de la organización, las desviaciones de los resultados previstos o favorables condiciones que ofrecen una ventaja con resultado beneficioso. Los auditores deberían verificar que la revisión de la gestionación incluya la consideración de todos los elementos b) a g) enumerados en la evidencia de auditoría de A.6.3. Los auditores también deberían confirmar que los resultados de la revisión por la dirección incluyen decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambios en el SGSI.
A.7 Mejora (ISO/IEC 27001:2013, clausula 10)	
A.7.1 No conformidad y acción correctiva (ISO/IEC 27001:2013, 10.1)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 7.5, 8.1, 10.2
Definiciones relevantes de ISO/IEC 27000	Corrección, acción correctiva, efectividad, no conformidad.
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) la naturaleza de las no conformidades y cualquier acción posterior tomada; b) los resultados de cualquier acción correctiva; c) resultados de monitoreo y medición; d) programa (s) de auditoría y los resultados de la auditoría; e) los resultados de la revisión por la dirección; f) los requisitos de las partes interesadas relevantes para la seguridad de la información; g) los cambios en el SGSI generados por acciones correctivas.

Guía práctica de auditoría	Los auditores deberían confirmar que: a) la organización responde encontrando no conformidades y requiriendo acciones correctivas cuando los requisitos ISO/IEC 27001 e SGSI (incluidos los operativos) no se cumplen; b) la no conformidad y la acción correctiva incluye tomar medidas para corregir la situación, examinar la causa y determinar si existen otras ocurrencias o si existen potencialmente en otro lugar para que se puedan tomar medidas para prevenir la recurrencia; c) la respuesta de la organización cubre la evaluación de las acciones tomadas para confirmar que se logró el resultado deseado, y la evaluación del SGSI para determinar si los cambios están justificados para evitar futuros eventos de no conformidades similares; d) la documentación de la no conformidad, la acción correctiva y los resultados se crean y controlan de acuerdo con los requisitos de información documentada (véase ISO/IEC 27001:2013, 7.5).
Documentos de respaldo	
A.7.2 Mejora continua (ISO/IEC 27001:2013, 10.2)	
Subcapítulos ISO/IEC 27001 relacionadas	ISO/IEC 27001:2013, 5.1, 5.2, 6.1, 6.2, 7.1, 8.1, 9.1, 9.2, 9.3, 10.1
Definiciones relevantes de ISO/IEC 27000	Mejora continua, efectividad, desempeño
Evidencia de auditoría	La evidencia de auditoría se puede obtener a través de información documentada u otra información sobre: a) la naturaleza de las no conformidades y cualquier acción posterior tomada, incluida la notificación de acciones correctivas; b) los resultados de cualquier acción correctiva; c) resultados de monitoreo y medición; d) programa (s) de auditoría y los resultados de la auditoría; e) los resultados de la revisión por la dirección;

	f) los requisitos de las partes interesadas relevantes para la seguridad de la información; g) evaluación y decisión sobre eventos e incidentes de seguridad de la información (véase ISO/IEC 27001:2013, A.16.1.4).
Guía práctica de auditoría	Los auditores deberían confirmar que la organización realiza su actividad recurrente para mejorar los resultados medibles de la idoneidad, adecuación y efectividad del SGSI. Los auditores deberían revisar y verificar que la mejora continua implica hacer cambios en el diseño y la implementación del SGSI para mejorar la capacidad de la organización para lograr la conformidad con los requisitos del SGSI y cumplir con sus objetivos y compromisos de política. Los auditores deberían confirmar mediante auditoría que la organización: a) desarrolla una implementación para lograr esta mejora, que incluye, pero no se limita a: 1) tomar medidas para abordar los riesgos y las oportunidades (véase ISO/IEC 27001:2013, 6.1); 2) establecer objetivos (véase ISO/IEC 27001:2013, 6.2); 3) actualizar los controles operativos (véase ISO/IEC 27001:2013, 8.1), teniendo en cuenta las nuevas tecnologías, métodos o información; 4) analizar y evaluar el desempeño (véase ISO/IEC 27001:2013, 9.1); b) realiza auditorías internas (véase ISO/IEC 27001:2013, 9.2); c) realiza revisiones de gestión (véase ISO/IEC 27001:2013, 9.3); d) detecta las no conformidades e implementa acciones correctivas (véase ISO/IEC 27001:2013, 10.1); e) evalúa y revisa periódicamente su SGSI de acuerdo con los requisitos de monitoreo, medición, análisis y evaluación (ISO/IEC 27001:2013, 9.1) y auditoría interna (ISO/IEC 27001:2013, 9.2) y revisión de la gestionación (ISO/IEC

	27001:2013, 9.3) para identificar oportunidades de mejora y planificar acciones apropiadas debería tomarse de acuerdo con acciones para abordar riesgos y oportunidades (ISO/IEC 27001:2013, 6.1), objetivos y planificación para alcanzarlos (ISO/IEC 27001:2013, 6.2) y planificación y controles operativos (ISO/IEC 27001:2013, 8.1).

BIBLIOGRAFÍA

[1] *ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*

[2] *ISO/IEC 17024, Conformity assessment — General requirements for bodies operating certification of persons*

[3] *ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements*

[4] *ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls*

[5] *ISO/IEC 27003:2017, Information technology — Security techniques — Information security management systems — Guidance*

[6] *ISO/IEC 27004, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] *ISO/IEC 27005, Information technology — Security techniques — Information security risk management*

[8] *ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[9] *ISO/IEC TS 27008, Information technology — Security techniques — Guidelines for the assessment of information security controls*

[10] *ISO/IEC 27021:2017, Information technology — Security techniques — Competence requirements for information security management systems professionals*

[11] *ISO 31000:2018, Risk management — Guidelines*

[12] IAF MD1, 2018, IAF Mandatory Document for the Audit and Certification of a Management system Operated by Multi-Site Organization, International Accreditation Forum. [viewed 2019- 01-01]. Available at https://www.iaf.nu/articles/Mandatory_Documents_/38