



Norma Internacional

ISO 19011

Directrices para la auditoría de los sistemas de gestión

Guidelines for auditing management systems

**Cuarta edición
2026-05**

Sample Document

get full document from standards.iteh.ai

Publicado por la Secretaría Central de ISO en Ginebra, Suiza, como traducción oficial en español avalada por el *Translation Management Group*, que ha certificado la conformidad en relación con las versiones inglesa y francesa.

Número de referencia
ISO 19011:2026(es)

© ISO 2026

Sample Document

get full document from standards.iteh.ai



DOCUMENTO PROTEGIDO POR COPYRIGHT

© ISO 2026

Todos los derechos reservados. Salvo que se especifique de otra manera o se requiera en el contexto de su implementación, no puede reproducirse ni utilizarse ninguna parte de esta publicación bajo ninguna forma y por ningún medio, electrónico o mecánico, incluidos el fotocopiado, o la publicación en Internet o una Intranet, sin la autorización previa por escrito. La autorización puede solicitarse a ISO en la siguiente dirección o al organismo miembro de ISO en el país del solicitante.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Publicado en Suiza
Versión en español publicada en 2026

Traducción oficial

© ISO 2026 – Todos los derechos reservados

Índice

Página

Prólogo	v
Prólogo de la versión en español	vi
Introducción	vii
1 Objeto y campo de aplicación	1
2 Referencias normativas	1
3 Términos y definiciones	1
4 Principios de auditoría	5
4.1 Generalidades.....	5
4.2 Integridad.....	5
4.3 Presentación imparcial.....	5
4.4 Debido cuidado profesional.....	6
4.5 Confidencialidad.....	6
4.6 Independencia.....	6
4.7 Enfoque basado en la evidencia.....	6
4.8 Enfoque basado en el riesgo.....	6
5 Gestión de un programa de auditoría	7
5.1 Generalidades.....	7
5.2 Establecimiento de los objetivos del programa de auditoría.....	10
5.3 Determinación y evaluación de los riesgos y oportunidades del programa de auditoría.....	10
5.4 Establecimiento del programa de auditoría.....	11
5.4.1 Roles y responsabilidades de las personas responsables de la gestión del programa de auditoría.....	11
5.4.2 Competencia de las personas responsables de la gestión del programa de auditoría.....	12
5.4.3 Establecimiento del alcance del programa de auditoría.....	12
5.4.4 Determinación de los recursos del programa de auditoría.....	13
5.5 Implementación del programa de auditoría.....	14
5.5.1 Generalidades.....	14
5.5.2 Definición de los objetivos, el alcance y los criterios para una auditoría individual.....	14
5.5.3 Selección y determinación de los métodos de auditoría.....	15
5.5.4 Selección de los miembros del equipo auditor.....	15
5.5.5 Asignación de responsabilidades al líder del equipo auditor para una auditoría individual.....	16
5.5.6 Gestión de los resultados del programa de auditoría.....	17
5.5.7 Gestión de registros relacionados con la auditoría.....	18
5.6 Seguimiento del programa de auditoría.....	18
5.7 Revisión y mejora del programa de auditoría.....	19
6 Realización de una auditoría	20
6.1 Generalidades.....	20
6.2 Inicio de la auditoría.....	20
6.2.1 Generalidades.....	20
6.2.2 Establecimiento del contacto con el auditado.....	20
6.2.3 Determinación de la viabilidad de la auditoría.....	20
6.3 Preparación de las actividades de auditoría.....	21
6.3.1 Realización de la revisión de la información documentada.....	21
6.3.2 Planificación de la auditoría.....	21
6.3.3 Asignación de las tareas al equipo auditor.....	23
6.3.4 Preparación de la información documentada para la auditoría.....	23
6.4 Realización de las actividades de auditoría.....	23
6.4.1 Generalidades.....	23
6.4.2 Asignación de los roles y las responsabilidades de los guías y los observadores.....	24
6.4.3 Realización de la reunión de apertura.....	24

ISO 19011:2026(es)

6.4.4	Comunicación durante la auditoría	25
6.4.5	Acceso a la información de auditoría	26
6.4.6	Revisión de la información documentada durante la auditoría	26
6.4.7	Recopilación y verificación de la información	26
6.4.8	Generación de los hallazgos de la auditoría	27
6.4.9	Determinación de las conclusiones de la auditoría	28
6.4.10	Realización de la reunión de cierre	28
6.5	Preparación y distribución del informe de la auditoría	29
6.5.1	Preparación del informe de la auditoría	29
6.5.2	Distribución del informe de la auditoría	30
6.6	Finalización de la auditoría	30
6.7	Realización de las actividades de seguimiento de la auditoría	31
7	Competencia y evaluación de los auditores	31
7.1	Generalidades	31
7.2	Determinación de la competencia del auditor	32
7.2.1	Generalidades	32
7.2.2	Comportamiento personal	32
7.2.3	Conocimientos y habilidades	33
7.2.4	Logro de la competencia del auditor	35
7.2.5	Logro de la competencia del líder del equipo auditor	36
7.3	Establecimiento de los criterios de evaluación del auditor	36
7.4	Selección del método apropiado de evaluación del auditor	36
7.5	Realización de la evaluación del auditor	37
7.6	Mantenimiento y mejora de la competencia del auditor	37
Anexo A (informativo)	Orientación adicional destinada a los auditores para planificar y realizar las auditorías	38
Bibliografía	50

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase www.iso.org/directives).

ISO llama la atención sobre la posibilidad de que la implementación de este documento pueda conllevar el uso de una o varias patentes. ISO no se posiciona respecto a la evidencia, validez o aplicabilidad de los derechos de patente reivindicados. A la fecha de publicación de este documento, ISO no había recibido notificación de que una o varias patentes pudieran ser necesarias para su implementación. No obstante, se advierte a los usuarios que esta puede no ser la información más reciente, la cual puede obtenerse de la base de datos de patentes disponible en www.iso.org/patents. ISO no será responsable de la identificación de parte o la totalidad de dichos derechos de patente.

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html.

Este documento ha sido elaborado por el Comité de Proyecto ISO/PC 302, *Directrices para la auditoría de los sistemas de gestión*, en colaboración con el Comité Técnico CEN/CLC/JTC 1, *Criterios relativos a los organismos de evaluación de la conformidad*, del Comité Europeo de Normalización (CEN), de conformidad con el Acuerdo de cooperación técnica entre ISO y CEN (Acuerdo de Viena).

Esta cuarta edición anula y sustituye a la tercera edición (ISO 19011:2018) que ha sido revisada técnicamente.

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

- ampliación de la orientación sobre métodos de auditoría remota mediante la introducción de la orientación contenida en la Especificación Técnica ISO/IEC TS 17012;
- ampliación del [Anexo A](#) para proporcionar orientación sobre los métodos de auditoría remota y las ubicaciones virtuales.

Cualquier comentario o pregunta sobre este documento deberían dirigirse al organismo nacional de normalización del usuario. En www.iso.org/members.html se puede encontrar un listado completo de estos organismos.

Prólogo de la versión en español

Este documento ha sido traducido por el Grupo de Trabajo *Spanish Translation Task Force* (STTF) del Comité Técnico ISO/CASCO, *Comité para la evaluación de la conformidad*, en el que participan representantes de los organismos nacionales de normalización y otras partes interesadas, para lograr la unificación de la terminología en lengua española en el ámbito de la evaluación de la conformidad.

Este documento ha sido validado por el ISO/TMBG/*Spanish Translation Management Group* (STMG) conformado por los siguientes países: Argentina, Bolivia, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, República Dominicana, México, Panamá, Paraguay, Perú y Uruguay.

Sample Document

get full document from standards.iteh.ai

Introducción

Desde la publicación de la tercera edición de este documento en 2018, se han publicado varias normas de sistemas de gestión en nuevos campos. Muchas de ellas tienen una estructura común, requisitos esenciales, términos comunes y definiciones esenciales idénticos. Como resultado, es necesario considerar un enfoque más amplio para la auditoría de los sistemas de gestión, así como proporcionar una orientación más genérica.

Este documento proporciona orientación que puede aplicarse para auditar con respecto a una serie de criterios de auditoría (de manera separada o combinada) incluyendo, pero sin limitarse a:

- los requisitos especificados en una o más normas de sistemas de gestión;
- las políticas, los procesos y los requisitos especificados por la organización u otras partes interesadas pertinentes;
- los requisitos legales y reglamentarios;
- uno o más procesos del sistema de gestión definidos por la organización y/o por otras partes;
- los planes de sistemas de gestión relacionados con la provisión de resultados específicos de un sistema de gestión (por ejemplo, el plan de la calidad, el plan de proyecto).

Este documento proporciona orientación para todas las organizaciones, independientemente de su tamaño y tipo, y para auditorías de distintos alcances. Esto incluye aquellas realizadas por equipos de auditoría grandes, típicamente de organizaciones grandes, y aquellas realizadas por auditores individuales, ya sea en organizaciones grandes o pequeñas. Esta orientación debería adaptarse según sea apropiado al alcance y la complejidad del programa de auditoría.

Este documento se concentra en las auditorías internas (de primera parte) y las auditorías realizadas por las organizaciones a sus proveedores externos y a otras partes interesadas externas (de segunda parte). Este documento también puede ser útil para las auditorías externas realizadas con fines distintos a una certificación de sistemas de gestión de tercera parte. La Norma ISO/IEC 17021-1 proporciona requisitos para la auditoría de sistemas de gestión para la certificación de tercera parte; aunque este documento puede proporcionar orientación adicional de utilidad (véase la [Tabla 1](#)).

Tabla 1 — Tipos distintos de auditoría

Primera parte	Segunda parte	Tercera parte
Auditoría interna	Auditoría externa de proveedor	Auditoría de certificación o evaluación de acreditación
	Auditoría realizada por la parte interesada externa de una organización	Auditoría legal, reglamentaria o similar

La Especificación Técnica ISO/IEC TS 17012 aborda la necesidad creciente de métodos de auditoría remota. Su propósito es dar orientación para la implementación eficaz de los métodos de auditoría remota, apoyando al mismo tiempo los principios generales de auditoría que se señalan en este documento.

Para simplificar la legibilidad de este documento, se prefiere la forma singular de “sistema de gestión”, pero el lector puede adaptar la implementación de la orientación a su propia situación. Esto también aplica al uso de “persona” y “personas”, “auditor” y “auditores”.

Se pretende que este documento se aplique a un amplio rango de usuarios potenciales, incluyendo auditores, organizaciones que implementan sistemas de gestión y organizaciones que necesitan realizar auditorías de sistemas de gestión por razones contractuales o reglamentarias. La orientación dada en este documento puede aplicarse por los usuarios al desarrollar sus propios requisitos relacionados con auditorías.

La orientación en este documento también puede usarse con el propósito de la autodeclaración, y puede ser útil para organizaciones involucradas en la formación, la titulación y la certificación de personas que participan en el programa de auditoría.

ISO 19011:2026(es)

La orientación en este documento pretende ser flexible. Como se indica en varios puntos del texto, el uso de esta orientación puede diferir dependiendo del tamaño y el nivel de madurez del sistema de gestión de una organización. También deberían considerarse la naturaleza y la complejidad de la organización que se va a auditar, así como los objetivos y el alcance de las auditorías que se van a realizar.

Este documento adopta el enfoque de auditoría combinada cuando se auditan juntos dos o más sistemas de gestión de distintas disciplinas. Cuando estos sistemas están integrados en un único sistema de gestión, los principios y procesos de auditoría son los mismos que para una auditoría combinada (a veces denominada "auditoría integrada").

Sample Document

get full document from standards.iteh.ai

Directrices para la auditoría de los sistemas de gestión

1 Objeto y campo de aplicación

Este documento da orientación sobre la auditoría de los sistemas de gestión, incluyendo los principios de la auditoría, la gestión de un programa de auditoría y la realización de auditorías de sistemas de gestión, así como orientación sobre la evaluación de la competencia de las personas que participan en el proceso de auditoría. Estas personas incluyen a aquellas responsables de la gestión del programa de auditoría, los auditores y los equipos auditores.

Es aplicable a todas las organizaciones que necesitan planificar y realizar auditorías de sistemas de gestión o gestionar un programa de auditoría.

La aplicación de este documento a otros tipos de auditorías es posible, siempre que se preste especial atención a la competencia específica necesaria y los objetivos a lograr.

2 Referencias normativas

No hay referencias normativas en este documento.

3 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes:

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

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

3.1 auditoría

proceso (3.25) sistemático, independiente y documentado para obtener *evidencias objetivas* (3.9) y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los *criterios de auditoría* (3.8)

Nota 1 a la entrada: Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por la propia organización o en su nombre.

Nota 2 a la entrada: Las auditorías externas incluyen lo que se denomina generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tales como los clientes o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes, tales como las que otorgan la certificación/registro de *conformidad* (3.21) o agencias gubernamentales y autoridades reguladoras.

[FUENTE: ISO 9000:2026, 3.12.1, modificado — Se ha añadido “documentado” y “objetivas” en la definición. Se han sustituido las Notas a la entrada.]

3.2 auditoría combinada

auditoría (3.1) llevada a cabo conjuntamente a un único *auditado* (3.14) en dos o más *sistemas de gestión* (3.19)

[FUENTE: ISO 9000:2026, 3.12.2, modificado — Se ha eliminado la Nota 1 a la entrada.]

3.3

auditoría conjunta

auditoría (3.1) llevada a cabo a un único *auditado* (3.14) por dos o más organizaciones auditoras

[FUENTE: ISO 9000:2026, 3.12.3]

3.4

método de auditoría remota

método utilizado para realizar actividades de auditoría desde cualquier lugar distinto de la ubicación del *auditado* (3.14)

Nota 1 a la entrada: Los métodos de auditoría remota pueden utilizarse en combinación con los métodos *in situ* para lograr una *auditoría* (3.1) completa y eficaz.

Nota 2 a la entrada: Los métodos de auditoría remota pueden utilizarse para ubicaciones virtuales, es decir, cuando una organización realiza un trabajo o proporciona un servicio utilizando un entorno virtual, lo que permite a las personas ejecutar *procesos* (3.25) independientemente de su ubicación física.

Nota 3 a la entrada: Los métodos de auditoría remota pueden ser utilizados por el *auditor* (3.16) en un sitio del *auditado* para auditar otro sitio.

[FUENTE: ISO/IEC TS 17012:2024, 3.1]

3.5

programa de auditoría

acuerdos para un conjunto de una o más *auditorías* (3.1) planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico

3.6

alcance de la auditoría

extensión y límites de una *auditoría* (3.1)

Nota 1 a la entrada: El alcance de la auditoría incluye generalmente una descripción de las ubicaciones físicas (véase 3.4, Nota 2 a la entrada) y virtuales, las funciones, las unidades de la organización, las actividades y los *procesos* (3.25), así como el periodo de tiempo cubierto.

3.7

plan de auditoría

descripción de las actividades y de los detalles acordados de una *auditoría* (3.1)

3.8

criterios de auditoría

conjunto de *requisitos* (3.24) usados como una referencia frente a la cual se compara la *evidencia objetiva* (3.9)

Nota 1 a la entrada: Si los criterios de auditoría son requisitos legales (incluyendo los reglamentarios), las palabras “cumplimiento” o “incumplimiento” se utilizan a menudo en un *hallazgo de la auditoría* (3.11).

Nota 2 a la entrada: Los requisitos pueden incluir políticas, procedimientos, instrucciones de trabajo, requisitos legales, obligaciones contractuales, normas de la industria, etc.

3.9

evidencia objetiva

datos que respaldan la existencia o veracidad de algo

Nota 1 a la entrada: La evidencia objetiva puede obtenerse por medio de la observación, medición, ensayo u otros medios.

[FUENTE: ISO 9000:2026, 3.8.6, modificado — Se ha eliminado la Nota 2 a la entrada.]

3.10

evidencia de la auditoría

registros, declaraciones de hechos o cualquier otra información que sea pertinente para los *criterios de auditoría* (3.8) y que es verificable

3.11

hallazgo de la auditoría

resultados de la evaluación de la *evidencia de la auditoría* (3.10) recopilada frente a los *criterios de auditoría* (3.8)

Nota 1 a la entrada: Los hallazgos de la auditoría indican *conformidad* (3.21) o *no conformidad* (3.22).

Nota 2 a la entrada: Los hallazgos de la auditoría pueden conducir a la identificación de *riesgos* (3.20), oportunidades para la mejora o el registro de buenas prácticas.

Nota 3 a la entrada: Si los criterios de auditoría se seleccionan a partir de los requisitos legales o los requisitos reglamentarios, el hallazgo de la auditoría se denomina “cumplimiento” o “incumplimiento”.

3.12

conclusión de la auditoría

resultado de una *auditoría* (3.1), tras considerar los objetivos de la auditoría y todos los *hallazgos de la auditoría* (3.11)

3.13

cliente de la auditoría

organización o persona que solicita una *auditoría* (3.1)

Nota 1 a la entrada: En el caso de una auditoría interna, el cliente de la auditoría también puede ser el *auditado* (3.14) o las personas que gestionan el *programa de auditoría* (3.5). Las solicitudes de una auditoría externa pueden provenir de fuentes como autoridades reguladoras, partes contratantes o clientes existentes o potenciales.

[FUENTE: ISO 9000:2026, 3.12.4, modificado — Se ha añadido la Nota 1 a la entrada.]

3.14

auditado

organización que es auditada en su totalidad o partes

3.15

equipo auditor

una o más personas que llevan a cabo una *auditoría* (3.1) con el apoyo, si es necesario, de *expertos técnicos* (3.17)

Nota 1 a la entrada: A un *auditor* (3.16) del equipo auditor se le designa como auditor líder del mismo.

Nota 2 a la entrada: El equipo auditor puede incluir auditores en formación.

3.16

auditor

persona que lleva a cabo una *auditoría* (3.1)

3.17

experto técnico

<auditoría> persona que aporta conocimiento o experiencia específicos al *equipo auditor* (3.15)

Nota 1 a la entrada: El conocimiento o experiencia específicos son los relacionados con la organización, la actividad, *proceso* (3.25), producto, servicio o disciplina a auditar, el idioma o la cultura.

Nota 2 a la entrada: Un experto técnico del equipo auditor no actúa como *auditor* (3.16).

3.18

observador

persona que acompaña al *equipo auditor* (3.15) pero que no actúa como un *auditor* (3.16) ni como un *experto técnico* (3.17)

3.19

sistema de gestión

conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas y objetivos, así como *procesos* (3.25) para lograr estos objetivos

Nota 1 a la entrada: Un sistema de gestión puede tratar una sola disciplina o varias disciplinas, por ejemplo, gestión de la calidad, gestión financiera o gestión ambiental.

Nota 2 a la entrada: Los elementos del sistema de gestión establecen la estructura, los roles y las responsabilidades, la planificación, la operación, las políticas, las prácticas, las reglas y las creencias de la organización, así como sus objetivos y los procesos para lograr esos objetivos.

Nota 3 a la entrada: El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

[FUENTE: ISO 9000:2026, 3.4.2, modificado — Se han añadido ejemplos en la Nota 1 a la entrada. Se ha ampliado la Nota 2 a la entrada. Se han eliminado las Notas 3 y 4 a la entrada.]

3.20

riesgo

efecto de la incertidumbre

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

Nota 2 a la entrada: Incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad.

Nota 3 a la entrada: Con frecuencia el riesgo se caracteriza por referencia a eventos y consecuencias potenciales, o a una combinación de estos.

Nota 4 a la entrada: Con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la probabilidad asociada de que ocurra.

[FUENTE: ISO 9000:2026, 3.7.2, modificado — Se ha eliminado la Nota 5 a la entrada.]

3.21

conformidad

cumplimiento de un *requisito* (3.24)

[FUENTE: ISO 9000:2026, 3.5.9]

3.22

no conformidad

incumplimiento de un *requisito* (3.24)

[FUENTE: ISO 9000:2026, 3.5.13]

3.23

competencia

capacidad para aplicar conocimiento y habilidades con el fin de lograr los resultados previstos

[FUENTE: ISO 9000:2026, 3.10.6]

3.24

requisito

necesidad o expectativa establecida, generalmente implícita u obligatoria

Nota 1 a la entrada: “Generalmente implícita” significa que es habitual o práctica común para la organización y las partes interesadas que la necesidad o expectativa bajo consideración esté implícita.

Nota 2 a la entrada: Un requisito especificado es el que está declarado, por ejemplo, en información documentada.

[FUENTE: ISO 9000:2026, 3.5.1, modificado — Se han eliminado las Notas 3, 4 y 5 a la entrada.]

3.25

proceso

conjunto de actividades interrelacionadas o que interactúan que utilizan entradas para proporcionar un resultado previsto

[FUENTE: ISO 9000:2026 3.3.1, modificado — Se ha eliminado “o transforman” y se ha añadido “previsto” en la definición. Se han eliminado las Notas a la entrada.]

3.26

desempeño

resultado medible

Nota 1 a la entrada: El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño se puede relacionar con la gestión de actividades, *procesos* ([3.25](#)), productos, servicios, sistemas u organizaciones.

[FUENTE: ISO 9000:2026, 3.7.3]

3.27

eficacia

grado en el que se realizan las actividades planificadas y se logran los resultados planificados

[FUENTE: ISO 9000:2026, 3.7.17]

4 Principios de auditoría

4.1 Generalidades

La auditoría se caracteriza por depender de varios principios. Estos principios deberían ayudar a hacer de la auditoría una herramienta eficaz y fiable en apoyo de las políticas y controles de gestión, proporcionando información sobre la cual una organización puede actuar para mejorar su desempeño. La adhesión a esos principios es fundamental para proporcionar conclusiones de la auditoría que sean pertinentes y suficientes, y para permitir a los auditores, que trabajan independientemente, alcanzar conclusiones similares en circunstancias similares.

La orientación dada en los [Capítulos 5](#) a [7](#) se basa en los siete principios señalados en los apartados [4.2](#) a [4.8](#).

4.2 Integridad

La integridad es el fundamento de la profesionalidad.

Los auditores y las personas que gestionan un programa de auditoría deberían:

- a) desempeñar su trabajo de forma ética, con honestidad y responsabilidad;
- b) emprender actividades de auditoría solo si son competentes para hacerlo;
- c) desempeñar su trabajo de manera imparcial, es decir, permanecer ecuanímenes y sin sesgo en todas sus acciones;
- d) ser sensibles a cualquier influencia que se pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

4.3 Presentación imparcial

La presentación imparcial es la obligación de informar con veracidad y exactitud.

Los hallazgos, conclusiones e informes de la auditoría deberían reflejar con veracidad y exactitud las actividades de auditoría. Se debería informar de los obstáculos significativos encontrados durante la

auditoría y de las opiniones divergentes sin resolver entre el equipo auditor y el auditado. La comunicación debería ser veraz, exacta, objetiva, oportuna, clara y completa.

4.4 Debido cuidado profesional

El debido cuidado profesional es la aplicación de diligencia y juicio al auditar.

Los auditores deberían proceder con el debido cuidado, independientemente de la importancia de la tarea que desempeñan y la confianza depositada en ellos por el cliente de la auditoría y por otras partes interesadas. Un factor importante al realizar su trabajo con el debido cuidado profesional es tener la capacidad de hacer juicios razonados en todas las situaciones de la auditoría.

4.5 Confidencialidad

La confidencialidad es la seguridad y privacidad de la información.

Los auditores deberían proceder con discreción en el uso y la protección de la información adquirida en el curso de sus actividades de auditoría. La información de la auditoría no debería usarse inapropiadamente para beneficio personal del auditor o del cliente de la auditoría, o de modo que perjudique los intereses legítimos del auditado. Este principio incluye el tratamiento apropiado de la información sensible o confidencial.

4.6 Independencia

La independencia es la base para la imparcialidad de la auditoría y la objetividad de las conclusiones de la auditoría.

Los auditores deberían ser independientes de la actividad que se audita siempre que sea posible, y en todos los casos deberían actuar de una manera libre de sesgo y conflicto de intereses. Los auditores deberían mantener la objetividad a lo largo del proceso de auditoría para asegurarse de que los hallazgos y las conclusiones de la auditoría están basados solo en la evidencia de la auditoría.

Cuando no resulte posible que los auditores internos sean independientes de la actividad que se audita, deberían hacerse todos los esfuerzos para eliminar el sesgo y fomentar la objetividad.

4.7 Enfoque basado en la evidencia

El enfoque basado en la evidencia es el método racional para alcanzar conclusiones de la auditoría fiables y reproducibles en un proceso de auditoría sistemático.

La evidencia de la auditoría debería ser verificable. Debería basarse en muestras de la información disponible, ya que una auditoría se lleva a cabo durante una duración especificada y con recursos finitos. Debería aplicarse un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que puede depositarse en las conclusiones de la auditoría.

4.8 Enfoque basado en el riesgo

El enfoque basado en el riesgo es un enfoque de auditoría que considera los riesgos y oportunidades.

El enfoque basado en el riesgo debería influir sustancialmente en la planificación y la implementación del programa de auditoría, y en la planificación, la realización y la presentación de informes de auditoría a fin de asegurar que las auditorías se centran en asuntos que son importantes para el cliente de la auditoría y para alcanzar los objetivos del programa de auditoría.

5 Gestión de un programa de auditoría

5.1 Generalidades

Debería establecerse un programa de auditoría. Este puede incluir auditorías que traten una o más normas de sistemas de gestión u otros requisitos, realizadas por separado o en combinación (auditoría combinada).

La extensión de un programa de auditoría debería basarse en el tamaño y la naturaleza del auditado, así como en la funcionalidad, la complejidad, el tipo de riesgos y oportunidades, el alcance y el nivel de madurez de los sistemas de gestión que se van a auditar.

La funcionalidad del sistema de gestión puede ser aún más compleja en el caso de múltiples ubicaciones o cuando hay funciones importantes contratadas externamente.

Debería prestarse especial atención a dónde se toman las decisiones importantes y al diseño, planificación y revisión del programa de auditoría.

El programa de auditoría debería adaptarse de acuerdo con el tamaño y la complejidad de la organización.

A fin de comprender el contexto del auditado, el programa de auditoría debería tener en cuenta los siguientes aspectos de la organización:

- los objetivos organizacionales;
- las cuestiones externas e internas pertinentes;
- las necesidades y expectativas de las partes interesadas pertinentes;
- la aplicación de tecnología, como herramientas digitales;
- los requisitos de seguridad y confidencialidad de la información.

A la hora de asignar recursos y métodos al programa de auditoría, debería darse prioridad a los asuntos del sistema de gestión con mayor riesgo inherente y menores niveles de desempeño.

Deberían asignarse personas competentes para gestionar el programa de auditoría (véase [5.4.2](#)).

El programa de auditoría debería incluir la información e identificar los recursos que permitan que las auditorías se realicen de forma eficaz dentro de los periodos de tiempo especificados. Esta información debería incluir lo siguiente:

- a) los objetivos del programa de auditoría (véase [5.2](#));
- b) los riesgos y oportunidades asociados con el programa de auditoría (véase [5.3](#)) y las acciones para abordarlos;
- c) el alcance (extensión, límites, ubicaciones) de cada auditoría dentro del programa de auditoría;
- d) el calendario (número/duración/frecuencia) de las auditorías;
- e) los tipos de auditoría, tales como internas o externas;
- f) los criterios de auditoría;
- g) los métodos de auditoría a emplear, incluyendo los métodos de auditoría remota (véase el [Capítulo A.16](#));
- h) los criterios para seleccionar al equipo auditor (líder del equipo auditor, auditores y, según sea necesario, expertos técnicos);
- i) los criterios para la participación de observadores, según sea pertinente;
- j) el contexto de la organización sobre la base de cuestiones externas e internas;
- k) la información documentada pertinente.